

## **ABSTRACT:**

This thesis is based around the questions of appropriateness and effectiveness of international measures against terrorist financing and internet transactions after the United States declared the ‘Financial War on Terror’ in the wake of 9/11, through comparing three example countries, and expands significantly on the research previously carried out in this area by the candidate.<sup>1</sup> This thesis provides an overview of the interpretation of the 1999 UN Convention for the Suppression of the Financing of Terrorism and questions whether it is applied uniformly. The main research focus is on the success or failure of subsequent legislative frameworks to combat terrorist financing generated and channelled via the Internet. Furthermore, the thesis aims to provide some recommendations in the concluding remarks on international cooperation when tackling the financial crime of terrorist financing. Here, ‘effective’ and ‘appropriate’ are defined through the case law applied by each jurisdiction, as well as the comments and criticisms surrounding their use, including through peer reviews from other countries examining their legislative mechanisms and interpretation of the 1999 UN Convention via the Financial Action Task Force.

By using doctrinal and comparative research, the thesis aims to show that an international response to Internet governance is required, in order to both increase effective enforcement of the 1999 Convention to online transactions, as well as improve the appropriateness of current cyber laws, including data surveillance and website filtration, so that UN Member States adhere to two important principles of the Universal Declaration of Human Rights 1948: that of privacy and of freedom of expression. The thesis responds to academic and US/UK Government thought that the Internet should

---

<sup>1</sup> Bensted, G. *Terrorist Financing and the Internet; dot com danger* (2012) 21 Information and Communications Technology Law 237.

not be governed by the UN, by highlighting significant gaps in the current application of cyber law, as well as the steady erosion of human rights. Furthermore, it will examine the evolution of the financing of terrorism, from the large transactions seen in 9/11, to the recent spate of terrorist attacks which have cost very little to carry out. As these transactions are unlikely to alert suspicious transaction reporting requirements under the 1999 Convention, this thesis aims to provide an analysis of alternative options available to governments and whether the lack of a definition of terrorism is hampering international efforts to disrupt and deter terrorist financing raised through the Internet.

## **Chapter One: Introduction**

*There was a time when people believed that the Internet was another world, but now people realise it's a tool that we use in this world<sup>2</sup>*

### **1.1. The evolution of terrorism**

Terrorism is a nebulous crime. It destroys communities through violence and subsequently heightens security by individual governments, yet there is no international definition as to what it is.<sup>3</sup> Therefore, some countries view it as a violent act or preparation for a violent act,<sup>4</sup> others see it as an assault on their social or religious norm.<sup>5</sup> As was famously defined in the book, *Harry's Game*, in 1975, “*one man's terrorist is another man's freedom fighter*”.<sup>6</sup> This rings true in today's climate, whereby those who shout their discontent with the status quo are potentially viewed with suspicion by governments. In the age of information, where it is commonplace to work, to bank and to socialise online, this quotation becomes more acute. Governments, public services, financial institutions, employers and friends are all able to find information

---

<sup>2</sup> Sir Tim Berners-Lee, inventor of the World Wide Web, BBC News (31 December 2003) *Web's Inventor Gets Knighthood* <<http://news.bbc.co.uk/1/hi/technology/3357073.stm>> accessed November 2016.

<sup>3</sup> No fewer than 9 UN Conventions are used to define terrorism. See the Annex to A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999) - UN Treaty Series 1973 *Convention for the Suppression of Unlawful Seizure of Aircraft* (16 December 1970); 974 UN Treaty Series 177 *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (23 September 1971); A/RES/3166 (XVIII) *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (14 December 1973); A/RES/34/146 *International Convention against the Taking of Hostages* (17 December 1979); INFCIRC/274 *Convention on the Physical Protection of Nuclear Material* (3 March 1980); 474 UN Treaty Series 1990 No. 14118 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (24 February 1988); 1678 UN Treaty Series 1992 No.29004 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (10 March 1988); 1678 UN Treaty Series 1992 No.29004 *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf* (10 March 1988); A/RES/52/164 *International Convention for the Suppression of Terrorist Bombings* (UN General Assembly) (15 December 1997).

<sup>4</sup> See chapter three, 3.2.1.1.

<sup>5</sup> See chapter six, 6.2.1.

<sup>6</sup> Seymour, G. *Harry's Game* (1st Edn. Corgi, 1975).

about an individual at the click of a button, and instant communications have now become the norm.

It is these tools, such as online banking, virtual currencies and the communications system which terrorists have used to their advantage. The most recent and prominent terrorist organisation, the Islamic State of Iraq and the Levant (ISIL),<sup>7</sup> showed their technological knowledge almost immediately, using social media networks such as Twitter, to publish their business plan,<sup>8</sup> issue threats to Western cities in the name of ‘jihad’<sup>9</sup> - and to recruit potential followers to their cause.<sup>10</sup>

Since September 11<sup>th</sup> 2001, (9/11), the most devastating attack on US soil since Japan bombed Pearl Harbour in 1941,<sup>11</sup> and the largest loss of life in a single terrorist attack,<sup>12</sup> both terrorism and the sources of its financing have been at the centre of international regulation. Yet, acts of terrorism date back millennia,<sup>13</sup> through the Assyrian empire, “*whose brutal methods of reprisal were intended to crush the spirit and break the will*”.<sup>14</sup> This eventually evolved to ‘anarchy’ during the 19<sup>th</sup> Century, most notably in the Paris Commune during 1871, when anarchists communicated their acts

---

<sup>7</sup> Islamic State of Iraq and the Levant, aka Islamic State, aka Islamic State of Iraq ash Sham, aka Daesh.

<sup>8</sup> Whitehead, T. (Daily Telegraph, 19 June 2014) *Isis operating like a multinational company* <<http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10911412/Isis-operating-like-a-multi-national-company.html>> accessed November 2016.

<sup>9</sup> At its height during the capture of Mosul in 2014, ISIL sent out 40,000 tweets in a single day; Irshaid, F. (BBC News, 19 June 2014) *How Isis is spreading its message online* <<http://www.bbc.co.uk/news/world-middle-east-27912569>> accessed November 2016; Neumann, P. R. *Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s* (ICSR 26 January 2015) <<http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>> accessed November 2016.

<sup>10</sup> Berger, J.M. *Tailored Online Interventions: The Islamic State's Recruitment Strategy* (Combating Terrorism Center, 23 October 2015) <<https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy;>> accessed November 2016.

<sup>11</sup> *9-11 Commission Report* (22 July 2004), 339-340 <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016.

<sup>12</sup> Johnstons Archive *Deadliest Terrorist Attacks Worldwide* (July 2016) <<http://www.johnstonsarchive.net/terrorism/wrjp255i.html>> accessed November 2016.

<sup>13</sup> To the Mesopotamian and Assyrian empires, see Chaliand, G. & Blin, A. *The History of Terrorism: From Antiquity to al-Qaeda* (1<sup>st</sup> Edn. University of California Press, 2007), vii.

<sup>14</sup> *ibid*.

and used dynamite to further their aims,<sup>15</sup> and terrorist acts leading to revolution in the early 20<sup>th</sup> Century.<sup>16</sup> Since then, modern forms of terrorism did not appear until the late 1960s, although Chaliand and Blin point out that there are four dates which terrorism historians point to: 1968, 1979, 1983 and 2001.<sup>17</sup> In 1968, Palestinians started the act of terrorism as a publicity stunt,<sup>18</sup> in 1979, the overthrow of the Iranian government was a high point for radical Shi'ite Islamism and marked the beginning of the Russia/Afghanistan conflict, from which al-Qaeda grew,<sup>19</sup> and 1983 saw the beginning of suicide bombings in Beirut, which led to the withdrawal of Western troops.<sup>20</sup> Furthermore, the UK saw a rise in domestic terrorism during this period, with the Irish Republican Army (IRA) carrying out numerous bomb attacks during the 1970s and 1980s, for example, in Birmingham, Guildford and Brighton.<sup>21</sup> Nevertheless, 9/11 was the first time terrorism transcended international borders, using the global financial system and communications via the Internet to finance and prepare the acts.

## **1.2. Financial Crime and the issue of Terrorist financing**

Financial crime itself has been mired in history. However, in the Twentieth Century, it had evolved from Ponzi schemes in the 1920s<sup>22</sup> to the money laundering of the Mafia between the 1930s and the 1980s,<sup>23</sup> and then onwards to the insider trading by the

---

<sup>15</sup> ibid Chaliand, G. & Blin, A. *The History of Terrorism; From Antiquity to al-Qaeda* (1<sup>st</sup> Edn. University of California Press, 2007), 123-125.

<sup>16</sup> ibid Chapter 8.

<sup>17</sup> ibid 221.

<sup>18</sup> ibid.

<sup>19</sup> ibid.

<sup>20</sup> ibid.

<sup>21</sup> BBC News (4 March 2001) *The IRA Campaigns in England* <<http://news.bbc.co.uk/1/hi/uk/1201738.stm>> accessed November 2016.

<sup>22</sup> US Securities and Exchange Commission *Ponzi Schemes* <<https://www.sec.gov/answers/ponzi.htm>> accessed November 2016.

<sup>23</sup> See in general Raab, S. *Five Families: The Rise, Decline, and Resurgence of America's Most Powerful Mafia Empires* (1<sup>st</sup> Edn. Chyrisalis Books Group, 2006).

end of the 1980s.<sup>24</sup> In the UK, financial crime is dryly defined as “*fraud or dishonesty; misconduct in, or misuse of information relating to, a financial market; or handling the proceeds of crime.*”<sup>25</sup> Yet financial crime has developed further than this. It is no longer restricted to the ‘white collar crime’ defined by Sutherland in the 1940s,<sup>26</sup> nor is it the laundering of vast profits from the criminal underbelly of the Five Mafia Families in New York.<sup>27</sup> Instead, it is fast becoming a few clicks of a mouse or a swiped screen to carry out a fraudulent transaction and is also becoming more intertwined with the running of terrorist organisations. For example, when ISIL produced its business plan in 2014,<sup>28</sup> this highlighted a number of similarities between a terrorist organisation and a company, including an annual report, albeit based on the number of deaths it had caused in 2013.<sup>29</sup> This also offers an insight into the modern terrorist organisation; there is a leader, or Chief Executive Officer,<sup>30</sup> a media officer, recruitment teams and a Treasurer, who handles the group’s finances. Once examining how a terrorist organisation operates and to view it as a business, as it needs finances to survive, it is easier to view it from the prism of financial crime.

---

<sup>24</sup> For example, Ivan Boesky was a Wall Street trader was imprisoned for making bets on the stock exchange based on insider tips *United States v. Boesky* 674 F.Supp. 1128 (1987). NB. It appeared with the financial crisis of 2008 that this had turned full circle – see in general Ryder, N. *The Financial Crisis and White Collar Crime The Perfect Storm?* (Edward Elgar, 2014).

<sup>25</sup> Financial Services and Markets Act 2000 c.8, s. 6(3)(a)-(c).

<sup>26</sup> Sutherland, E.H. *White Collar Crime* (New York: The Dryden Press, 1949).

<sup>27</sup> Raab, S. *Five Families: The Rise, Decline, and Resurgence of America's Most Powerful Mafia Empires* (1<sup>st</sup> Edn. Chyrisalis Books Group, 2006).

<sup>28</sup> Whitehead, T. (Daily Telegraph, 19 June 2014) *Isis operating like a multinational company* <<http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10911412/Isis-operating-like-a-multi-national-company.html>> accessed November 2016.

<sup>29</sup> *ibid.*

<sup>30</sup> In al-Qaeda’s case, Osama bin Laden before he died, and in ISIL’s case Abu Bakr Al-Baghdadi.

As will be outlined in further depth in chapter three, terrorist financing is a financial crime distinct from money laundering.<sup>31</sup> Whereas the goals of terrorist financing and money laundering are the same; that is, to conceal money,<sup>32</sup> the reasons behind concealing currency is inherently different. While money launderers seek to turn money derived from crime into ‘clean’ cash, terrorist financiers use monies derived from a wide variety of sources, to finance illegal, rather than legal aims. Essentially, terrorist financing has been described as ‘*reverse money laundering*’,<sup>33</sup> yet this simple terminology belies the complexities terrorist financing; that it is derived from both licit and illicit sources, and can use money laundering as a way to place substantial funding into the global financial system.

9/11 was a defining moment for the international community in terms of the focus on terrorist financing. Prior to this event, the financing of terrorism garnered little international attention, with just 42 out of 193 Members signing the UN’s Convention for the Suppression of the Financing of Terrorism 1999, and only four ratifying it.<sup>34</sup> It was the impetus of the United States which brought terrorist financing to the fore after 9/11, when President George W. Bush declared not only a War on Terrorism, but a ‘Financial War On Terrorism’ less than two weeks after 9/11, by freezing the assets of 27 entities which were suspected of financing terrorism.<sup>35</sup> Ultimately,

---

<sup>31</sup> Chapter three, 3.2.

<sup>32</sup> Donohue, L.K. *Anti Terrorist Finance in the United States and the United Kingdom* (2005-2006) 27 Michigan Journal of International Law 303, 393.

<sup>33</sup> Cassella, S.D. *Reverse Money Laundering* (2003) 7(1) Journal of Money Laundering Control 92, 92.

<sup>34</sup> 1999 Convention on the Suppression of the Financing of Terrorism <<https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf>> accessed November 2016.

<sup>35</sup> The Whitehouse Archives *President Freezes Terrorists’ Assets* (24 September 2001) <<https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>> accessed November 2016.

the US brought the issue of terrorist financing before the attention of the United Nations Security Council. This approach caused the UN Security Council to issue a binding Resolution under Article VII of the UN Charter, 1373,<sup>36</sup> just seventeen days after 9/11; a seminal moment in the history of counter-terrorism. It is therefore a core part of this thesis to understand and note that both the 1999 Convention and UN Security Council 1373 set out the international basis for counter-terrorist financing, and that they are binding on each Member State of the UN.

### **1.3. The use of the Internet by terrorists**

9/11 also proved to be a watershed moment for the realisation that terrorists were using the Internet to communicate and finance their acts. The 9/11 Commission subsequently found that the terrorists had used coded emails to message each other in the lead up to the World Trade Center attacks, with Mohamed Atta sending the other hijackers the following email, referring to the targets, and stating that *'the semester begins in three more weeks. We've received 19 confirmations for the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering...'*<sup>37</sup> This email provided the impetus of a plethora of laws aimed at stemming the flow of terrorist financing, as well as increasing levels of surveillance on Internet communications.

The use and accessibility of the Internet has rapidly increased over the last twenty years, from a 1% Internet penetration rate in 1995 to 40% in 2016.<sup>38</sup> Two

---

<sup>36</sup> UN Security Council Resolutions S/RES/1368 (2001) Counter-Terrorism Implementation Task Force (12 September 2001) and S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts (28 September 2001).

<sup>37</sup> Weimann, G. *www.terror.net – How Modern Terrorism uses the Internet* (March 2004) Special Report 116 United States Institute of Peace 10.

<sup>38</sup> Internet Live Stats *Internet Users* (2016) <<http://www.internetlivestats.com/internet-users/>> accessed November 2016.



billion more people now have access to the Internet than in 2005, rising from one billion in 2005 to three billion in 2016.<sup>39</sup> This astonishing rise in access has all occurred without a comprehensive international legal framework to oversee use of the Internet, indeed reflecting the values of the inventors, who said “[t]he original idea of the web was that it should be a collaborative space where you can communicate”.<sup>40</sup> Consequently, this has made it an attractive way of channelling funds for illicit and illegal purposes. With virtual anonymity and speed, as noted above, using the Internet has not escaped the attention of terrorist organisations. Moreover, the Internet is a cost-effective medium to broadcast terrorist ideologies and to recruit followers on a worldwide basis.<sup>41</sup> However, it was the 2002 Bali Bomber, Imam Samudra, who spread publicly the fact that the Internet was an attractive way to raise financing for terrorist acts.<sup>42</sup> In a chapter of Samudra’s autobiography, “*Me against the Terrorist!*” entitled “*Hacking, Why Not?*”, Samudra outlined that the Internet could be a valuable source of terrorist financing, urging his readers to commit cybercrime, to raise funds in furtherance of Jihad.<sup>43</sup> Since then, the international community has been focused on evolving technology and terrorists’ abuse of it, readily deploying surveillance techniques to disrupt and deter terrorist communications.

Therefore, the thesis examines the effects of data surveillance and whether some countries are taking levels of surveillance to an intrusive level, which potentially

---

<sup>39</sup> *ibid.*

<sup>40</sup> Sir Tim Berners-Lee, inventor of the World Wide Web, (BBC News 31 December 2003) *Web’s Inventor Gets Knighthood* <<http://news.bbc.co.uk/1/hi/technology/3357073.stm>> accessed November 2016.

<sup>41</sup> Conway, M. *Terrorism and the Internet: Core Governance and Issues* (2007) 3 Disarmament Forum 23, 25.

<sup>42</sup> Sipress, A. (Washington Post 16 December 2004) *An Indonesian’s Prison Memoir Takes Holy War Into Cyberspace* <<http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>> accessed November 2016.

<sup>43</sup> *ibid.*

impinges on basic human rights of privacy and freedom of expression under Articles 12 and 19 of the Universal Declaration of Human Rights.<sup>44</sup>

#### 1.4. Structure of the thesis

With terrorist uses of the Internet in mind, Hinnen detailed four main ways in which terrorists use the Internet to finance their aims:<sup>45</sup>

- (i) *Direct solicitation of donations;*
- (ii) *Use of charitable organisations;*
- (iii) *Online crimes;*
- (iv) *Communications.*

Hinnen, at the time of writing his work, was also a Trial Attorney with the United States Department of Justice's Computer Crime & Intellectual Property Section,<sup>46</sup> therefore he was uniquely placed to comment on the US reaction towards terrorist financing and Internet transactions immediately after 9/11. His work, *The Cyber-Front in the War on Terrorism*, covers many aspects of terrorist use of the Internet, yet when writing about the ways in which terrorist financing is raised he understood that terrorist financing was an inherently distinct crime from money laundering, stating that "*terrorists and terrorist organizations are not profit motivated. Their ultimate goal is not to amass wealth; it is rather to inflict harm and instill terror.*"<sup>47</sup> Furthermore, Hinnen's article is split into two areas under each heading; prevention and investigation, and prosecution. By understanding the measures from the begin-

---

<sup>44</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A) <<http://www.un.org/en/universal-declaration-human-rights/>> accessed November 2016.

<sup>45</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 9.

<sup>46</sup> *ibid.*

<sup>47</sup> *ibid* 8.

ning to the end of a legal process, this provides the author the ability to analyse effectiveness and appropriateness of mechanisms governing the financing of terrorism and use of the Internet by terrorists.

Hinnen's definitions of online terrorist financing form the basis of this thesis, providing comparative resonance and continuity between the examples used. Under three headlines, combining direct solicitation of donations and communications, each chapter will be structured as follows:

- (i) *Direct solicitations through websites and electronic communications;*
- (ii) *Using legitimate sources such as charities and financial institutions as a front for raising and channelling finances;*
- (iii) *Cybercrime including cyberlaundering and online fraud.*

However, Hinnen's work was published in 2002, when just over half a billion people in the world had access to the Internet.<sup>48</sup> The evolution of the Internet and the resulting measures governments have put in place to combat terrorist financing online since then has moved substantially further forward. Additionally, Hinnen had outlined his arguments about the effectiveness of only one country's legislation, the US, and had not fully weighed up privacy issues against the need for effective investigations. Because the Internet is inherently global, this thesis has a comparative outlook, through using three case studies and examining the international legislation which overarches both terrorist financing and Internet freedom. It also aims to take Hinnen's work further, showing that there are potential solutions available to disrupt and deter terrorist financing through the means he described.

---

<sup>48</sup> Internet Live Stats *Internet Users* (2002) <<http://www.internetlivestats.com/internet-users/>> accessed November 2016.

Within this thesis, the effectiveness and appropriateness of each example jurisdictions' measures against terrorist financing will be examined, in order to evaluate the best and worst practice examples of counter-terrorist financing measures. Furthermore, the use of this structure will enable the author to gauge whether there are any effective and appropriate solutions towards the problems encountered when applying these measures, making recommendations in the concluding chapter.

#### **1.4.1. The definition of effectiveness**

Here, effectiveness is relatively straightforward to explain in the context of law. Essentially, effectiveness is how successfully a legal doctrine can be applied to the initial aims of a domestic or international body. Black's Law Dictionary therefore succinctly defines this as "[t]he closeness of actual results achieved to meeting expectations",<sup>49</sup> ignoring expenditure and focusing on results, whilst weighing these against expectations over time. As a result, there must first be a "baseline" by which results can be calculated to conclude whether legislative reaction has been effective or not. In this instance, 9/11 has been chosen because this is the moment at which national and international legislatures changed in their focus onto terrorism and disrupting terrorist finances. Therefore, measurements of results and their effectiveness can be taken before and after this moment in time to find out how effective they have been.

##### **1.4.1.1. Effectiveness in the context of counter-terrorist financing**

However, the construct of effectiveness goes further than just listing convictions and the level of assets frozen – which can be easily identified – it is also an examination of the example countries' legal systems to find out whether they were and still are

---

<sup>49</sup> Black's Law Dictionary, <<https://thelawdictionary.org/effectiveness/>> accessed March 2018.

prepared for the evolution of terrorism, as well as the way in which terrorist organisations finance their operations. As such, several areas are examined in order to judge the level of effectiveness and to ensure that a full account can be made of international efforts to combat terrorism and its financing.

1. *The actions of the international community and comparative countries on the issue of terrorist financing prior to 9/11;*
2. *The aims of the international community after 9/11, and if they have been achieved;*
3. *The changes the international community and each country had to make to their legal responses to terrorism and its financing after 9/11 and the scope of international standards;*
4. *Whether the subsequent changes made to legislation were able to conform with international standards of combating terrorist financing through identifying gaps and weaknesses in national legislation;*
5. *Examples of best and worst practice through case studies;*
6. *Whether the international standards have been applied to their fullest extent; how they are applied and how they are enforced if not.*

It is therefore important to compare how previous legislative actions had to change after 9/11 to tackle what became an international crime which spanned numerous countries, to find out how effective they have become. For example, the intentions of the Clinton administration in the wake of the 1998 attacks on the U.S. Embassies in Kenya and Tanzania were the same as those of the Bush administration after 9/11: to disrupt terrorist finances and to cripple terrorist organisations such as Al-Qaeda. However, due to the lack of primary focus for the Federal Bureau of Investigation and

Central Intelligence Agency on the problem of terrorist financing,<sup>50</sup> while a substantial amount of Taliban assets had been frozen (\$254million),<sup>51</sup> Clinton's aim of attacking the structure of Al-Qaeda through financial sanctions had been unsuccessful. This was mainly because there was limited support from international financial institutions, as well as a lack of international sanctions or co-operation on non-compliance.<sup>52</sup> After 9/11, Bush extended his executive powers to deal with terrorist financing<sup>53</sup> as well as taking the issue to the United Nations, making it an international obligation for Member States and their financial institutions to tackle. On the surface, therefore, one can draw the conclusion that Clinton's measures were half-heartedly applied and did not carry the weight of all U.S. law enforcement agencies or the international community with it, leaving the U.S. wide open to the first attack on its soil since Pearl Harbour. More subtly, however, when one also examines the post-9/11 measures by the U.S., the reaction to this event on terrorism in the 16 years afterwards may also not have been so effective in tackling the pervasiveness of terrorist financing. Therefore, to provide an overall picture of effectiveness, it is necessary to identify the aims both pre- and post-9/11 to explain the comparative point and assess whether they have been achieved.

The aims of the international community, as well as domestic legislatures, must also be outlined to gauge whether the legal response to the financing of terrorism has been effectively applied. Within the context of counter-terrorist financing, the

---

<sup>50</sup> Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*, 4 <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018.

<sup>51</sup> Hardister, A.D *Can We Buy a Peace on Earth: The Price of Freezing Terrorist Assets in a Post-September 11 World* (2002) 28 N.C. J. Int'l L. & Com. Reg. 605, 609 Hardister, A.D, *Can We Buy a Peace on Earth: The Price of Freezing Terrorist Assets in a Post-September 11 World*, 28N.C. J. Int'l L. & Com. Reg.605 (2002), 609.

<sup>52</sup> *ibid.*

<sup>53</sup> *ibid.*

overall objectives of the international community can be seen in a combination of the 1999 UN Convention for the Suppression of the Financing of Terrorism<sup>54</sup> and its referral to the Declaration on Measures to Eliminate International Terrorism 1994,<sup>55</sup> General Assembly Resolution 51/210 of 17 December 1996,<sup>56</sup> as well as the UN Security Council's Resolutions in the immediate aftermath of 9/11.<sup>57</sup>

1. *An unequivocal condemnation of terrorism as criminal;*<sup>58</sup>
2. *All Member States to take steps to prevent and counteract, through domestic measures, financing of terrorists and terrorist organisations;*<sup>59</sup>
3. *International co-operation to prevent and suppress the financing of terrorism*<sup>60</sup>  
*through criminalisation of terrorist financing, freezing and confiscating assets, as well as preventative measures through financial institutions, businesses and professionals, and cross-border control of monetary instruments;*<sup>61</sup>
4. *Adoption of regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes;*<sup>62</sup>

---

<sup>54</sup> International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution A/RES/54/109 of 9 December 1999.

<sup>55</sup> General Assembly Resolution A/RES/49/60 Measures to eliminate international terrorism (9 December 1994).

<sup>56</sup> *ibid* A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999).

<sup>57</sup> For example, UN Security Council Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, which mandates a number of counter terrorist financing measures, to be elaborated on later in the thesis.

<sup>58</sup> General Assembly Resolution A/RES/49/60 Measures to eliminate international terrorism (9 December 1994).

<sup>59</sup> General Assembly Resolution A/RES/51/210 Measures to eliminate international terrorism (17 December 1996).

<sup>60</sup> *ibid* A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999).

<sup>61</sup> UN Security Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, [1].

<sup>62</sup> *ibid* General Assembly Resolution A/RES/51/210 Measures to eliminate international terrorism (17 December 1996).

5. *Intensifying and accelerating exchange of information concerning international movements of terrorist funds<sup>63</sup> in accordance with international and domestic law,<sup>64</sup>*
6. *Prosecution and punishment of perpetrators of terrorist financing.<sup>65</sup>*

As a result, these broad requirements can be employed as a basis on which to build an argument surrounding the effectiveness of the example countries' subsequent legislation, as well as the UN and international bodies' actions after 9/11. By using the core UN instrument to combat terrorist financing, the UN Convention for the Suppression of the Financing of Terrorism, as a measurement point, the question of effectiveness can be answered, because each jurisdiction is compared with the above aims and the minimum standards of the 1999 Convention.

#### **1.4.1.2. Effectiveness in the context of Internet transactions**

Furthermore, given that counter-terrorist financing rules are applicable to legitimate financial transactions generated via the Internet, these principles and aims can be applied in much the same manner when assessing their effectiveness in disrupting terrorist finances. Banking and transacting through legitimate financial institutions, including electronic transactions, are subject to the same financial rules, as set down by the UN and other international actors, so effectiveness can be judged when examining the basic international and national laws governing this area.

Nevertheless, effectiveness is less linear while examining the actions of Internet Service Providers on the solicitation of donations through websites and the sharing

---

<sup>63</sup> *ibid.*

<sup>64</sup> UN Security Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, [3].

<sup>65</sup> *ibid* A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999).



of electronic communications with state actors. Here, because there is no UN Security Council Resolution on the use of the Internet by terrorists or UN Convention to ensure minimum standards on Internet use, individual countries effectively make their own decisions on how far Internet surveillance goes, and there is no requirement for mutual legal assistance on cybercrime. As will be outlined under 1.4.2.2 of this chapter, this also affects the appropriateness element of the thesis. Therefore, the following questions should be asked when determining effectiveness of actions to prevent terrorist financing over the Internet:

1. *Is there international and regional law in this area?*
2. *Are there any mutual assistance agreements between the comparative countries to share information and provide legal assistance for acts of cybercrime?*
3. *In the absence of regional or international agreements on cybercrime, what applicable domestic legislation is in place in comparative countries?*
4. *Has this domestic or regional legislation helped to capture acts of terrorist financing over the Internet?*
5. *Are there any gaps in regional or domestic law which need to be addressed?*

By using these questions as a guide, the author will be able to determine whether the current issues facing individual jurisdictions when tracing Internet transactions should be resolved at an international level. Through an examination of both best practice and gaps in legislation, this could point the argument towards the necessity of international agreement on some form of regulation of the Internet. Specifically, and as will also be discussed in 1.4.2.2., the European Convention on Cybercrime is a regional agreement which does attempt to align domestic legislation and has been signed and ratified by countries outside of the Council of Europe, including the

United States, Canada and Australia.<sup>66</sup> Therefore, it can be used as a starting point for examining the effectiveness of international action (or lack thereof) on both cyber-crime in general and the use of the Internet by terrorist organisations.

Although, as the guidance notes to the Convention state,<sup>67</sup> it “*is not a treaty that is focused specifically on terrorism*”,<sup>68</sup> the substantive crimes arising from the Convention can be used as acts of terrorism, to facilitate terrorism and to support terrorism, including financially.<sup>69</sup> Furthermore, the Convention has mutual legal assistance tools in Article 14, which would ostensibly help countries who are dealing with terrorist financing as a cybercrime, or cybercrimes which involve terrorist financing. Therefore, areas such as electronic evidence collection,<sup>70</sup> preservation of data to use in criminal investigations,<sup>71</sup> and compelling evidence from Internet Service Providers to provide evidence and co-operate with law enforcement authorities<sup>72</sup>, are significant in determining the effectiveness of criminal investigations into terrorist financing and Internet transactions.

#### **1.4.2. The definition of appropriateness**

The definition of appropriateness is undoubtedly more complex and less easy to quantify than effectiveness. Black’s Law Dictionary defines appropriateness as “[a]cting

---

<sup>66</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001) <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>> accessed March 2018.

<sup>67</sup> Council of Europe Cybercrime Convention Committee *T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention*, adopted by the 16th Plenary of the T-CY (14-15 November 2016): <[file:///C:/Users/georg/AppData/Local/Microsoft/Windows/INetCache/IE/U960IG5U/T-CY\(2016\)11\\_GuidanceNote11\\_terrorism\\_V15adopted.docx.pdf](file:///C:/Users/georg/AppData/Local/Microsoft/Windows/INetCache/IE/U960IG5U/T-CY(2016)11_GuidanceNote11_terrorism_V15adopted.docx.pdf)> accessed March 2018.

<sup>68</sup> *ibid.*

<sup>69</sup> *ibid.*

<sup>70</sup> Cybercrime Convention Article 14(1)(c).

<sup>71</sup> *ibid* Article 16.

<sup>72</sup> *ibid* Article 21.

*appropriately or fitting the requirements that are asked of a party*”<sup>73</sup> and that ‘requirements’ are “[a]ny demands, constraints, needs, necessities needed to be met”.<sup>74</sup> However, this does not go quite far enough to highlight what legal standard should be met for a measure or action to be ‘appropriate’ when dealing with counter-terrorist financing and its application to Internet transactions. Clearly, there are many levels when dealing with appropriateness in the context of law and legal interpretation for counter-terrorism. For example, while Saudi Arabia may have domestic policies and decisions on counter-terrorism and Internet surveillance which may not be appropriate to and attract criticism from jurisdictions such as the United States or the United Kingdom,<sup>75</sup> it may well be working within the confines of either international regulation or its own legal interpretation and constitution. Additionally, the UN’s Universal Declaration of Human Rights,<sup>76</sup> which includes many important areas relevant to counter-terrorist financing and Internet transactions, such as the right to a private life<sup>77</sup> and freedom of opinion and expression,<sup>78</sup> is not binding on Member States. Therefore, as noted above, whereas one Member State and its agencies may respect the Declaration’s principles, others may not. As a result, it is necessary to not only examine appropriateness within the framework of international legislation in this area, but also resulting national legislation from international law; each country’s constitution; interpretation of domestic law by Government agencies and national courts’ interpretation of the legality of actions by the Government and national agencies when understanding their obligations.

---

<sup>73</sup> Black’s Law Dictionary: <<http://thelawdictionary.org/appropriateness/>> accessed March 2018.

<sup>74</sup> *ibid* <<http://thelawdictionary.org/requirements/>>.

<sup>75</sup> E.g. The case of Raif Badawi, an Internet blogger who was sentenced to 1,000 lashes and ten years imprisonment for ‘insulting Islam’. This is dealt with in further depth in Chapter Six.

<sup>76</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A).

<sup>77</sup> *ibid* Article 12.

<sup>78</sup> *ibid* Article 19.

As a result, several questions must be asked to narrow down the extent of appropriateness to find the legal standards which are part of counter-terrorism and Internet law:

1. *What is the scope of the international standard?*
2. *Does the measure or law subsequent to 9/11 meet with or breach international standards?*
3. *What is the scope of the comparative country's constitution and legal precedent set by domestic or regional courts?*
4. *Do the measures or laws subsequent to 9/11 meet with or breach the comparative country's constitution and legal precedent?*

#### **1.4.2.1. Appropriateness in the context of counter-terrorist financing**

As noted with effectiveness under 1.4, it is necessary first to examine the overarching international legal framework surrounding counter-terrorist financing, the 1999 UN Convention for the Suppression of the Financing of Terrorism,<sup>79</sup> which, as mentioned previously, provides the main basis for international and domestic action against terrorist financing conducted in more than one Member State.<sup>80</sup> This Convention also captures Internet transactions which are international by nature (i.e. crossing borders through ISPs based in different countries).<sup>81</sup> After the events of 9/11 and the emerging

---

<sup>79</sup> International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution A/RES/54/109 of 9 December 1999: <<http://www.un.org/law/cod/finterr.htm>> accessed November 2016.

<sup>80</sup> NB. Article 3 notes that the Convention will not apply to acts carried out in one Member State.

<sup>81</sup> E.g. The Financial Action Task Force, which interprets and enforces international standards on anti-money laundering and counter-terrorist financing, has as part of its Recommendation for member countries 'new technologies' under Recommendation 15, formerly Recommendation 8 – "*Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They*

picture of the way terrorists financed their acts, the UN Security Council passed Resolution 1373, which made it mandatory for Member States to become parties to the Convention, which entered into force in April 2002.<sup>82</sup> Therefore, many jurisdictions had to abide by those provisions which, as Gurulé notes,<sup>83</sup> were split into five categories:

- (i) *Freezing terrorist-related assets, domestically and internationally;*
- (ii) *Implementing and enforcing regulatory measures to prevent terrorists from abusing the global financial system;*
- (iii) *Implementing international standards on counter-terrorist financing;*
- (iv) *Prosecuting terrorist financiers and their facilitators;*
- (v) *Litigating civil tort actions brought by the victims of terrorist attacks.*<sup>84</sup>

While much of the Convention deals with appropriateness within the framework of domestic regulations, providing leeway for Member States as to their own interpretation of what is appropriate,<sup>85</sup> there are some limitations to these powers, as evidenced by some of the Articles, specifically those relating to extradition for crimes committed under the Convention, as well as mutual legal assistance. For example, the Convention states that there is no obligation to extradite or afford mutual legal assistance if the State Party believes that the request “*has been made for the purpose of*

---

*should take appropriate measures to manage and mitigate those risks*”. Full list of Recommendations available at the Financial Action Task Force website <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed November 2016.

<sup>82</sup> Security Council Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, r.3(d).

<sup>83</sup> Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008), 6.

<sup>84</sup> *ibid.*

<sup>85</sup> E.g. Article 4 states that each State Party will establish terrorist financing offences under Article 2 as criminal offences under (a), yet (b) notes that the offences must be made punishable “*by appropriate penalties which take into account the grave nature of the offences.*”, providing some leeway for States to determine what penalties should be necessary to punish terrorist financing.

*prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons*" under Article 15,<sup>86</sup> and Article 17 states that anyone who is taken into custody or is subject to proceedings under the Convention "*shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law.*"<sup>87</sup> Consequently, these provisions have some elements of human rights legislation which, by the very binding nature of the Convention, should be adhered to by all signatories in the context of mutual legal assistance and extradition, unless specific reservations have been made.<sup>88</sup>

Second, as noted above, the Convention does not explicitly cover appropriateness of domestic legislation on counter-terrorist financing. As is often the case, domestic legislation on counter-terrorism is part of national security measures, given the fast-paced nature of the crime and the need for preventing it from happening in the

---

<sup>86</sup> International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in resolution A/RES/54/109 of 9 December 1999.

<<http://www.un.org/law/cod/finterr.htm>> accessed November 2016.

<sup>87</sup> *ibid.*

<sup>88</sup> NB. No reservations to Articles 15 and 17 have been made, although there were concerns by a number of countries that, for example, the Arab Republic of Egypt's reservations limited the scope of Article 6 – see United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999)

<[https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=XVIII-11&chapter=18&lang=en](https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en)> accessed November 2016.

first place<sup>89</sup>. Therefore, the scope of what is appropriate in terms of an ordinary criminal investigation are stretched somewhat, including emergency legislation,<sup>90</sup> the ability of courts to sign off surveillance warrants,<sup>91</sup> as well as financial surveillance measures. Consequently, to look at the appropriateness of these measures must be within the context of the country's existing constitution, blackletter law and their interpretation by domestic courts, to find out whether there is a human rights element and, if so, whether this has been breached by subsequent measures.<sup>92</sup>

#### **1.4.2.2. Appropriateness in the context of Internet transactions**

It is more difficult to set appropriateness within the context of Internet transactions as, although many of the international standards on counter-terrorist financing can be

---

<sup>89</sup> For example, in the US, successive Presidents have used Executive Orders to investigate and freeze assets of terrorist groups and suspected individuals under the International Emergency Economic Powers Act of 1977, including 13,224 in 2001. There have been many controversies about Executive Orders as they allow the President to make major decisions or law without the consent of Congress, including in times of national security. While they are generally used to direct federal agencies and officials in the deliverance of Congressionally established laws or policies, there have been instances where they have been used to guide agencies contrary to Congressional intent. These are subject to judicial review and must adhere to the United States Constitution. However, in 1974, Executive Orders were so prevalent that the Senate Committee on National Emergencies and Delegated Emergency Powers was authorised to investigate the matter. The committee made several findings, including the fact that the United States had been governed under emergency rule since Franklin D. Roosevelt called a state of emergency in 1933. By 1999, thirteen states of emergency were still in place and Congress had not used its powers to terminate those emergencies. Branum, T.L. *President or King - The Use and Abuse of Executive Orders in Modern-Day America* (2002) Journal of Legislation: Vol. 2: Issue. 1, Article 9.

<sup>90</sup> For example, the USA PATRIOT Act of 2001 has a number of sunset clauses on controversial surveillance powers as they were introduced in a time of emergency, but these were reauthorised by Congress in 2006, 2010 and 2011 - USA PATRIOT Act Improvement and Reauthorization Act of 2005 (Pub. L. 109-177, 120 Stat. 192) (NB. 14 out of 16 provisions set to expire in 2006 were made permanent – only “roving wiretaps” on multiple telephone lines under §206 and stored records access under §215 had further sunset provisions); H.R. 3961ENR (2010), Public Law No. 111-114, which extended provisions until 28 February 2011; The PATRIOT Sunsets Extension Act of 2011 (Pub. L. 112-114, 125 Stat. 216) (50 U.S.C. 1801) extended provisions until 1 June 2015.

<sup>91</sup> For example, the US's USA PATRIOT Act allows warrantless surveillance for non-domestic communications, although the Foreign Intelligence Surveillance Court monitors this – see Chapter 4 for further information.

<sup>92</sup> NB. In the case of the United Kingdom, due to its lack of a written Constitution, one would also have to examine a mixture of regional legislation from the European Union, existing blackletter law and precedent set by national courts.

transplanted onto technological advances in banking, the surveillance of Internet communications as part of monitoring those transactions has no binding international legislation from the United Nations Security Council. However, as mentioned previously, another international instrument, which has been signed or ratified by 60 countries, including non-members,<sup>93</sup> is the Council of Europe's Budapest Convention 2001, or the Convention on Cybercrime. Here, the Convention would relate to the investigation of crimes committed via the Internet, including the financing of terrorism. Therefore, to apply the test of appropriateness, it is worthwhile to examine the Convention's regulations and set them against each country's measures on Internet surveillance. Of particular note is Article 15, which states that parties to the Convention will ensure that the establishment, implementation and application of powers under domestic law will "*provide for the adequate protection of human rights and liberties... and which shall incorporate the principle of proportionality*".<sup>94</sup> As will be discussed at length in chapter four, the issue of proportionality of Internet surveillance powers by individual countries is a factor in the measurement of appropriateness. As noted earlier, both the United States and the United Kingdom have signed and ratified the Convention, meaning that the tests of human rights such as privacy and freedom of expression can apply, as well as the proportionality of domestic legislation in carrying out investigations of Internet communications when tracing terrorist financing. Furthermore, the United States has enshrined in its Constitution the right to freedom of expression,<sup>95</sup> the right to privacy<sup>96</sup> and the right to a speedy and public trial,<sup>97</sup> and

---

<sup>93</sup> Council of Europe, Signatories to the Cybercrime Convention 2001, <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>> accessed 10 September 2017.

<sup>94</sup> *ibid.*

<sup>95</sup> Constitution of the United States 1787, First Amendment.

<sup>96</sup> Constitution of the United States 1787, Fourth Amendment.

<sup>97</sup> Constitution of the United States 1787, Sixth Amendment.



the United Kingdom is subject to the Human Rights Act 1998, which also enshrines the same rights.<sup>98</sup> Therefore, appropriateness is weighed against both countries' obligations under domestic, regional and international regulations.

With Saudi Arabia, the test of appropriateness must differ; it is not a signatory to the Convention on Cybercrime, nor does it apply the UN's Universal Declaration of Human Rights as it is not a signatory to the UN's International Convention on Civil and Political Rights 1966. Furthermore, there is no written penal code, with Saudi courts instead applying Shari'ah law to criminal acts.<sup>99</sup> However, as noted above, Saudi Arabia is a party to the 1999 Convention for the Suppression of the Financing of Terrorism, therefore is bound by the same international standards as the United States and the United Kingdom, including any human rights derived from its application to extradition and mutual legal assistance. Additionally, the UN Security Council's Resolution 1373, passed in the wake of 9/11, called upon Member States to become parties to "*as soon as possible to the relevant international conventions and protocols relating to terrorism*",<sup>100</sup> some of which again take into account the fact that there is no obligation for parties to the Convention to extradite or provide mutual legal assistance if they have grounds for believing that it is on the basis of political, philosophical, ideological, racial, ethnic or political opinion, rather than the predicate offences outlined in the Convention.<sup>101</sup> Consequently, freedom of expression and opinion by Saudi individuals in foreign states could be caught by these provisions, even if

---

<sup>98</sup> Human Rights Act 1998 c.42, Schedule 1, Part I, Articles 10 (freedom of expression), 8 (privacy) and 6 (right to a fair trial) respectively.

<sup>99</sup> MENAFATF Mutual Evaluation Report on Saudi Arabia, (25 June 2010) 15, para. 53, 16 para. 54 <[www.fatf-gafi.org](http://www.fatf-gafi.org)> accessed November 2016; Basic Law of 1992, Article 8.

<sup>100</sup> UN Security Council Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts s.3(d).

<sup>101</sup> A/RES/52/164 International Convention for the Suppression of Terrorist Bombings (15 December 1997) Article 12.

the Saudi Arabian Government objects, therefore it is worthwhile to use these standards to assess appropriateness. Furthermore, it is a member of the UN's Human Rights Council until 2019.<sup>102</sup> Therefore, some elements of appropriateness of its Internet surveillance measures regarding acts of terrorist financing can be weighed against its international obligations.

## **1.5 Structure of each Chapter**

As noted in 1.4 above, each comparative chapter is set against the points outlined by Hinnen. However, to effectively compare each judicial system, it is necessary to outline how the chapters are individually structured, to show the reader how and why each legislative principle has been introduced and whether they are appropriate and effective, as well as to highlight the established arguments about each approach towards counter-terrorist financing and Internet transactions or communications.

### **1.5.1 Chapter Three: Background to the international position on financial crime and regulation of the Internet before 9/11**

This chapter is the most important for the reader. Not only does it provide a history of efforts against terrorism, financial crime and computer crime, it lays the foundation for the arguments set out later in the thesis. Clearly, the chapter must be arranged into two main sections, to show the evolution of financial crime; as well as the advancement of 'computer crime' from hacking a mainframe into traditional crimes committed via the Internet, for example, money laundering and fraud. Therefore, the chapter is longer than the others, mainly since efforts in two distinct areas of law before 9/11

---

<sup>102</sup> United Nations High Commissioner for Human Rights *Current Membership of the Human Rights Council* <<http://www.ohchr.org/EN/HRBodies/HRC/Pages/CurrentMembers.aspx>> accessed November 2016.

have to be explained for each jurisdiction and married into the thesis' overall argument, namely:

- (i) ***Financial Crime*** – *an explanation of the development from money laundering by organised crime syndicates in the 1970s, to drug barons in the 1980s, and then towards financial crimes committed by terrorist organisations in the 1990s.*
- (ii) ***Computer crimes*** – *an explanation of the development from traditional forms of computer crime, such as hacking, to a more nuanced form of criminal activity via the Internet, namely using it as a tool to commit crimes and to transfer illicit profits.*

It is worthwhile to note here that the United States and the international community were unprepared for 9/11. By outlining what focus each authority had on both financial crime and technological advances, this bolsters the argument that 9/11 and its financing took each jurisdiction by surprise. Through understanding the background of financial crime, this shows the scale of the problem each jurisdiction and the United Nations were facing at the time of 9/11 and allows the author to show whether the reaction since 9/11 was effective and appropriate. Similarly, the findings of the 9/11 Commission and Samudra's thesis show that there was an endemic problem with the Internet - that it was, and still is, open to abuse by criminal entities.

#### **1.5.2. Chapter Four: The United States**

There are many reasons why the United States (US) is evaluated first. As has been outlined previously, it was the 'victim' of 9/11, had immense influence on the UN Security Council at the time and housed many of the world's most prolific Internet

Service Providers (ISPs), search engines, and social networking sites.<sup>103</sup> Within this chapter, the author aims to show that US lawmakers were mistaken in their attentions during the aftermath of 9/11. Whereas before the event of 9/11, the US had focused its legislative and investigative resources towards money laundering – whether generated through the Mafia or drug lords – the ensuing reaction underestimated the scale and the type of problem Al Qaeda posed. As noted before, money laundering and terrorist financing are inherently different forms of financial crime. The USA PATRIOT Act,<sup>104</sup> passed virtually immediately in the wake of 9/11, combined these two forms of financial crime without understanding their backgrounds or effects. Hence, the US reaction subsequent to 9/11 was poorly focused; while it managed to force the UN Security Council into action and spurred international reactions towards the ‘Financial War on Terror’, the fundamental lack of understanding that terrorist financing and money laundering are separate crimes has cost the US and the UN to a degree. Chapter four, comparing each of Hinnen’s ways of generating and channelling finances through the Internet, highlights how underprepared the United States truly was when combatting terrorist financing prior to 9/11 and how it failed to provide an adequate response after 9/11. This is combined with leaving ISPs and social networking sites to police themselves in the wake of 9/11, has caused significant problems for other jurisdictions who have to deal with the aftermath of propaganda, solicitation of donations to a terrorist organisation and many impressionable people to join ‘causes’ such as ISIL.

---

<sup>103</sup> E.g. Google and Facebook are based in California. Facebook has approximately 2 billion monthly users worldwide, as of 2017 Statista *Number of monthly active Facebook users worldwide as of 2nd quarter 2017 (in millions)* <<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>> accessed November 2017, and Google has 3.5 billion searches per day and 1.2 trillion searches per year worldwide Internet Live Stats *Google Search Statistics* (2016) <<http://www.internetlivestats.com/google-search-statistics/>> accessed November 2017.

<sup>104</sup> Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Pub. L. 107-56, 115 Stat. 272).

Additionally, the author will show that a core plank of the U.S.'s financial war on terror, the Suspicious Activity Report, which banks and other financial institutions use to identify and report suspicious transactions, may be outdated and cumbersome when dealing with terrorist financing and the plethora of electronic transactions which are conducted daily. The Suspicious Activity Report regime – used internationally to identify transactions relating to money laundering, fraud and terrorist financing – is based on patterns of transactions modelled on the money laundering offence of “smurfing” or layering small amounts of money into the formal financial system. As the author notes earlier within this chapter, terrorist financing is known as “reverse money laundering”, meaning that they are virtually untraceable using the Suspicious Activity Report regime, adding a further issue for tracing terrorist finances generated and funnelled through the Internet.

Moreover, the author aims to highlight that the surveillance measures employed by the U.S. were also ill-thought out, and potentially harmful for Internet users. Again, the author intends to show that USA PATRIOT Act was passed quickly and without consideration of its wide-ranging powers which had the ability to be intrusive and capture communications of innocent Internet users, and that they have been found to violate fundamental U.S. constitutional rights, without the recourse to judicial or independent oversight. While this may be effective in capturing the communications of potential terrorists and terrorist groups, the author wants to show that this has been at the cost of basic rights afforded to the U.S. population and beyond.

### **1.5.3. Chapter Five: The United Kingdom**

The United Kingdom (UK) is a key comparison country. Aside from having a similar legal system to the United States, as mentioned earlier, the UK is in the unique position

of having a long history of terrorism prior to 9/11, and that it had already implemented counter-terrorist financing strategies to combat this issue. The United Kingdom is also part of the European Union, therefore enjoys regional elements to the sharing of information pursuant to counter-terrorism but is bound by clear human rights obligations within that region, including the right to privacy.

Within chapter five, the author aims to highlight how effective the use of counter-terrorist financing plans has, or has not been, to combat terrorism. Unlike the United States, the United Kingdom clearly distinguishes the crimes of terrorist financing and money laundering, which is an important element of disrupting this form of financial crime. This enables the author to both compare each domestic reaction towards 9/11 and the issue of financing terrorism via the Internet. While the minimum standards of international counter-terrorist financing regulations also bind the UK, it can go further in their application due to existing legislation, meaning they are used more effectively to prevent the flow of this currency through the financial system. Additionally, the UK went further than the U.S. to combat the evolving issue of “cheap terrorism” – i.e. those acts which can be financed through minimal amounts of funding. Significantly, terrorism evolved from costing nearly half a million U.S. dollars to less than £1,000 in the 7/7 bombings, less than four years after 9/11, and then onwards to the 2013 murder of Fusilier Lee Rigby which would have cost less than £20 to carry out. This recognition by UK law enforcement authorities that terrorism evolves to evade financial constraints set by the international community is an important distinction, and the preventative actions taken after these events are ones which can be used by other domestic jurisdictions to combat the prevalence of terrorist financing.

However, the author also aims to show that the UK has fallen into the same traps as that of the United States: those of an over-use of the Suspicious Activity Report system to track terrorist financing through Internet transactions which may not be effective, as well as an over-reliance on surveillance, which may not be appropriate. Furthermore, the UK suffers from one great omission within its ability to counteract terrorist financing; that it is unable to produce intercept evidence within its prosecution cases. This means one of the main aims of the UN's 1999 Convention is essentially scuppered: to prosecute and punish perpetrators of terrorist financing.

The author also highlights that the UK, not being bound by a written constitution as the U.S. is, has gone far beyond this jurisdiction's actions to counter terrorism and its financing over the Internet. While this may be more effective, the UK has problems in showing the appropriateness of these plans to the European Union (EU) and jars somewhat with the more protective nature of the EU and the US towards freedom of speech and expression.

#### **1.5.4. Chapter Six: The Kingdom of Saudi Arabia**

This chapter examines combating terrorist financing since 9/11, from the position of an important country in the Middle East. Aside from the prominent connections to both the UK and the US through its trade in arms and security services, the overall contradiction between this relationship and the links of many of the 9/11 bombers and Saudi Arabia, including sources of their finance, makes this jurisdiction a key comparison for the author to make in determining the success or failure of the international reaction towards stemming the flow of terrorist finances. Additionally, there are further contradictions between the application of international law and its own religious legal system to prosecute criminal offences, Shari'ah. Unlike countries with similar

secular legal systems, such as the UK and the US, as well as Member States of the European Union, Saudi Arabia has to ensure that international legal requirements to combat terrorist financing are harmonised with fundamental constructs of Shari'ah, including its charitable system of *zakat*, which was found to be vulnerable to terrorist organisations after 9/11. Similarly, the rapidly increasing Internet penetration of the country, without binding international guidelines to oversee potential human rights violations, makes this jurisdiction's efforts to combat the problem of terrorist financing via the Internet a critical contrast with those of the US and the UK.

Within chapter six, the author illustrates how Saudi Arabia has implemented important elements of the 1999 UN Convention, and examines whether there have been any pitfalls within its application to Internet transactions, through for example, charitable donations. Theoretically, Saudi Arabia's Shari'ah law was considered to include terrorist financing as an offence prior to 9/11,<sup>105</sup> however, this was not used to any extent before the UN Security Council's Resolution 1373 was introduced after 9/11. Post-9/11, a significant report from the Middle East North Africa Financial Action Task Force in 2010 also showed that there were several gaps in Saudi Arabia's CTF regulation which hampered international aims to combat terrorist financing.<sup>106</sup> Therefore, the author aims to examine what, on the surface Saudi Arabia has promised since 9/11, and whether this has, in reality, helped to capture terrorist financiers who have used the Internet to channel and raise their funding.

Furthermore, by focusing on the way in which Saudi Arabia uses its Internet censorship tools, the author can make a comparison between all example nations, as well as the European Union, on their respective positions towards Internet censorship

---

<sup>105</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report on Saudi Arabia*, (25 June 2010) 37-38; 148.

<sup>106</sup> *ibid.*



and surveillance, and assess whether any are appropriate or effective when used to combat terrorist financing. Saudi Arabia is, as the author will highlight, at the strict end of the spectrum on Internet surveillance, while the European Union is more focused on the data protection of individuals. Between those two ends of the spectrum, both the UK and the US have enhanced capabilities to filter websites – in the UK’s case – and observe individual communications with recourse to secretive Foreign Intelligence Surveillance Courts, as in the US. Each of these, while legal in their own jurisdictions, may nevertheless have an impact on effectiveness and appropriateness. This further leads the author to be able to link these concerns with the final chapter – the United Nations and conclusion – and an assessment of whether it is now time to have a minimum set of legal standards on Internet regulation.

#### **1.5.5. Chapter Seven: The United Nations and International Organisations – Conclusion**

This chapter brings together the elements of the previous chapters though looking at the way in which the United Nations (UN) and other international organisations have been able to carry out the initial aims of the 1999 Convention since 9/11. Moreover, the glacial pace at which the UN moves to regulate areas such as financial crime has been out-manoeuvred by the speed at which criminals have adapted to new forms of technology to further their aims, which the author highlights clearly within this chapter. Due to the international nature of both the UN and Internet Service Providers, this should place the UN in a position to ensure that minimum legal standards on Internet regulation, yet it does not, despite the clear warning signs that terrorist organisations are using the Internet to plan and finance their actions since 9/11. This lack of action, the author aims to show, has resulted in markedly different actions towards disrupting

terrorist finances which are raised and channelled through the Internet, with some countries trying to formulate an effective and appropriate response without the co-operation of other jurisdictions, which either will not or cannot combat this type of financial crime. The author shows, within this chapter, that the UN's response thus far has been lacking, due to several fundamental reasons:

1. ***The lack of an international definition of terrorism*** meaning that countries who believe a terrorist organisation is planning its actions in another may not receive international co-operation due to differing definitions.
2. ***The lack of a binding resolution on cybercrime*** showing that efforts to curb terrorist financing over the Internet may become limited to single jurisdictions or regions as there is no international minimum standard for all Member States to adhere to.
3. ***That the International Convention on Human Rights is non-binding*** leaving it up to individual countries to assess whether their actions are appropriate and meaning that breaches of privacy or freedom of expression through Internet surveillance largely go unchecked by the international community.
4. ***No peer-to-peer assessments of counter-terrorist financing regulations*** – a useful tool for increasing the effectiveness of individual jurisdictions' actions on counter-terrorist financing and anti-money laundering is left to other international organisations such as the Financial Action Task Force to undertake.

This chapter therefore unpicks these difficulties from an international angle, as well as compare all three examples from an international view. The chapter further offers the author an opportunity to come up with solutions to these problems, using best practice examples from each jurisdiction, in order to come up with a workable solution to the growing and ever-present danger that the Internet is now being used by

terrorist organisations to avoid the stringent measures placed on formal financial institutions after 9/11. By doing so, the author will also be able to provide a holistic solution to an inherent problem which has been troubling the international community for well over a decade and to shut down one of the most prevalent ways of financing this modern evil.

## **Chapter Two: Methodology & Literature Review**

### **2.1. Introduction:**

It is important to discuss the differences between ‘methodology’ and ‘method’, as one is the underpinning ethos to the thesis and the other is a method of research used as to bolster and interpret this methodological standpoint. Henn et al point out that, while method refers to the tools available to collect evidence, methodology concerns the research strategy as *a whole*, including political, theoretical and philosophical implications.<sup>107</sup> This is an important distinction to make, because at a basic level, this thesis is part of a ‘growing field’ of comparative research on counter-terrorism since 9/11,<sup>108</sup> questioning and contextualising the measures of both national and international bodies in their response to financial crime and, in particular, counter-terrorist financing (CTF) since those events. Layered within this research is a focus on the use of the Internet to communicate and to transact, from the perspective of both licit and illicit sources. Consequently, it is first essential to understand that analysing terrorism and terrorist financing cannot be pinned down to one form of research – that, in fact, it must include several forms of method, combined, to provide a more robust picture of national and international measures in this subject area. As Roach states “*one of the great challenges of studying counter-terrorism laws is that they cross traditional disciplinary boundaries within academe and even within law...*”.<sup>109</sup> Behind these forms of research is the doctrinal methodology – it is inescapable for a thesis based on legal doctrine to be without this form of framework. With this outlook in mind, the research

---

<sup>107</sup> Henn, M. Weinstein, M and Foard, N. *A Short Introduction to Social Research* (1<sup>st</sup> Edn. 2006 SAGE Publications) 9.

<sup>108</sup> Roach, K. *The 9/11 Effect: Comparative Counter-Terrorism* (1<sup>st</sup> Edn. Cambridge University Press, 2011), 5.

<sup>109</sup> *ibid* 6.

strategy of this thesis is doctrinal; it examines the United Nations (UN) Convention of the Suppression of Terrorist Financing 1999 and subsequent UN Security Council Resolution 1373 of 2001, as well as the resulting legislation of each country. Therefore, not only must one examine CTF through an overall doctrinal methodology, but also research how legislation is applied and the effects it has through qualitative and comparative research methods, to establish patterns and, eventually, find solutions.

It is also important to note that these are areas which have only gathered pace in research since 9/11. Indeed, as Silke states, “[o]ne of the most notable findings in the previous reviews of the research literature was just how little research was focused on *al-Qaeda* in the ten years prior to 9/11.”<sup>110</sup> The impact of 9/11 was wide and varied: from the immediate legislative reforms<sup>111</sup> to the focus on its financing,<sup>112</sup> as well as increased surveillance on communications as more people started to use the Internet on a regular basis.<sup>113</sup> Yet, there must also be a focus on what happened beforehand. As Silke further states “[p]rior to 9/11, only 3.9 percent of articles examined non-contemporary terrorism... Yet this wider context is almost entirely ignored, as terror-

---

<sup>110</sup> Silke, A. *Contemporary terrorism studies: Issues in research: Critical Terrorism Studies: A New Research Agenda*, ed. Jackson, R., Breen Smyth, M., Gunning, J. (Routledge, 2009).

<sup>111</sup> For example, the USA PATRIOT Act was passed within weeks of 9/11 – it was passed by House of Congress by 357 to 66 votes on 25 October 2001 and passed by the Senate by 98 to 1; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 *European Journal of Law Reform* 137, 139; in the House it was passed by 357 Yeas to 66 Nays with 9 not voting/not present and passed by the Senate by 98 Yeas to 1 Nay with 1 not voting/not present <<http://www.govtrack.us/congress/bill.xpd?bill=h107-3162>> accessed November 2016.

<sup>112</sup> For example, the UN Security Council enacted Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, which was binding on all Member States, included the point that Member States shall ‘prevent and suppress the financing of terrorist acts’ under Article 1(a).

<sup>113</sup> For example, the use of PRISM by GCHQ and the National Security Agency to tap into Internet communications; Greenwald, G & MacAskill, E. (The Guardian, 7 June 2013) *NSA Prism program taps into user data of Apple, Google and others* <<http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>> accessed November 2016; Black, I. (The Guardian Newspaper, 10 June 2013) *NSA Spying Scandal: What we have learned* <<http://www.guardian.co.uk/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned>> accessed November 2016.

*ism research is increasingly driven by a need to provide a short-term, immediate assessment of current groups and threats.*”<sup>114</sup> Consequently, a large part of this research shows the actions of example countries and international organisations prior to 9/11, in order to contextualise the subsequent legislative measures and to answer the questions of effectiveness and appropriateness.

Within this chapter, a key aim is to outline why different methods are being used to answer the questions of effectiveness and appropriateness, including the use of qualitative, comparative, and doctrinal methodologies. This will be broken down into the overall rationale behind using each methodology, as well as an explanation behind choosing the three example countries and the UN, outlined in this thesis. Finally, there is also an analysis of the literature used, in order to show the evidence base used to support the arguments and conclusions made.

## **2.2. Rationale of using Doctrinal Methodology:**

At its very core, this thesis uses doctrinal methodology to show the outcomes of CTF after 9/11, as legislation and jurisprudence is often the first point of contact to understand the examples’ framework behind their application of CTF and Internet usage. Doctrinal law is often cited as the ‘expository’ form of research, being ‘[a] *synthesis of various rules, principles, norms, interpretive guidelines and values. It explains, makes coherent or justifies a segment of the law as part of a larger system of law.*’<sup>115</sup> From doctrinal law springs forth case law and the policies of each example used, partly answering the questions ‘why’ and ‘how’ they are applied. As Wendell Jr. asserted in the Path of Law “*if we want to know why a rule of law has taken its particular shape,*

---

<sup>114</sup> *ibid* Silke, A. Silke, A. *Contemporary terrorism studies: Issues in research: Critical Terrorism Studies: A New Research Agenda*, ed. Jackson, R., Breen Smyth, M., Gunning, J. (Routledge, 2009).

<sup>115</sup> Mann, T. (ed), *Australian Law Dictionary* (1<sup>st</sup> Edn. Oxford University Press, 2010) 197.

*and more or less if we want to know why it exists at all, we go to tradition.*"<sup>116</sup> Consequently, it is imperative to recognise which legal doctrine each example uses, to provide a comprehensive assessment, upon which conclusions and recommendations can be made.

Identifying the type of legal system each example uses is also an important starting point. As outlined in chapter three and will be expanded upon later in this chapter at 2.5, the legal differences between the United Kingdom (UK), the United States (US) and Kingdom of Saudi Arabia are clear. While the UK has an unwritten constitution, and case law has been founded on precedent, it must also apply a set of regional rules under the European Union (EU), which, being based on Napoleonic Codes, are inherently juxtaposed to the traditional legal system of the UK – with the sovereignty of Parliament and the rule of law<sup>117</sup> subservient to the decisions of EU institutions. This potentially causes a conflict between settled common law and the application of decisions by the Court of Justice of the EU (CJEU). Furthermore, while there are some similarities to the UK's legislative background, the US uses a written Constitution, by which it is bound, and federal law, therefore jurisprudence is more inflexible than that in the UK, being based on a narrow set of confines when interpreting constitutional questions. As a more marked comparison, Saudi Arabia has a highly religious legal system, Shari'ah law, based on religious principles set out in the Qur'an, meaning that its own legislative actions may be outdated and, in some circumstances, archaic when applied to monitoring new technologies.

---

<sup>116</sup> Wendell, O. *The Path of the Law* (1897) 10(8) Harvard Law Review 457.

<sup>117</sup> Dicey, A.V. *Introduction to the Law of the Constitution* (8<sup>th</sup> Edn. Oxford Press, 1915).

Above these, at an international level, the UN has a set of Resolutions and Conventions based on minimum standards, which potentially expose gaps in interpretation by Member States. Yet, these jurisdictions are bound to apply UN legal principles in the case of CTF, such as the 1999 Convention on the Suppression of the Financing of Terrorism, as well as UN Security Council Resolution 1373. It is important to note that this Resolution was agreed under Chapter VII of the UN Charter and is binding on all Member States of the UN. Therefore, it is key to be able to understand the differences before comparing how each jurisdiction applies the international standards expected of them by the UN. In the case of Internet regulation, there is no corresponding or binding UN instrument, meaning that each state is responsible for their own monitoring or filtration of Internet correspondence and content. Underlying these assessments, there must be several points which need to be answered to ensure that each is based on an equal footing – most importantly, the meaning of every legal provision, its context, and the decision-making which arises out the legal framework. By examining legislative provisions in this manner, and in combination with qualitative methodology, doctrinal methodology can be employed to find out what is used, why it is used and how it is applied.

### **2.3. Rationale of using Qualitative and Comparative Research Design methods:**

As Chynoweth explains, doctrinal research by itself is *“concerned with the discovery and development of legal doctrines for publication in textbooks or journal articles and its research questions take the form of asking ‘what is the law?’ in particular*



*contexts*”<sup>118</sup> which, by itself, offers too narrow a perspective in this context. Terrorism, by its very nature, is a global crime with significant effects on communities, therefore any study of it must have a qualitative method with comparative design underpinning its research. Qualitative research in this thesis provides the author with the flexibility to analyse and interpret basic legal tenets, including a completion of the ‘why’ and the ‘how’ of applying international measures on CTF and national measures on Internet surveillance, to support conclusions and recommendations, rather than just focusing on quantifying the results of a data collection exercise. Indeed, it would be difficult to quantify the ‘appropriateness’ of certain countries’ measures towards counter-terrorism and Internet communications, given that international law in these areas only ask for ‘minimum standards’.<sup>119</sup> Additionally, within this qualitative research method is the comparative research design. Bryman describes that this *‘implies that we can understand social phenomena better when they are compared in relation to two or more meaningfully contrasting cases or situations.’*<sup>120</sup> In the context of this thesis, as noted before, the issues of counter-terrorism and surveillance of Internet communications are international. As such, providing a ‘snapshot’ of Member States’ regulation and policies towards CTF and Internet use, and ending with the UN and international agencies’ measures, will give broader context to CTF and Internet transactions, as well as providing opportunities to discover best practice and critically analyse different approaches to this subject matter.

---

<sup>118</sup> Chynoweth, P. *Legal research in the built environment: A methodological framework* (Ruddock, L & Knight, A (eds.) *Advanced Research Methods in the Built Environment* 2008, Wiley-Blackwell), Ch. 3, 28-38.

<sup>119</sup> For example, the Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A) <<http://www.un.org/en/universal-declaration-human-rights/>> accessed November 2016.

<sup>120</sup> Bryman, A. *Social Research Methods* (2nd Edn. Oxford University Press, 2004), 53.

The events of 9/11 themselves showed through recruitment, planning, financing and exercise that a number of different countries, as well as global financial and communications systems, were used to carry out al-Qaeda's end goals. For example, in the aftermath of 9/11, it was shown that three of the pilots, Mohamed Atta, Ziad Jarrah and Marwan al Shehhi were based in Germany, forming the 'Hamburg Cell',<sup>121</sup> eventually beginning their training in Karachi after becoming more radicalised during their studies as students<sup>122</sup> and logging dozens of international trips for training and meetings in the lead up to 9/11, facilitated by al-Qaeda's Chief Financier, Khalid Sheik Mohammed.<sup>123</sup> The fourth pilot, Hani Hanjour, was originally from Saudi Arabia, yet had studied in the US during the 1990s, as well as learning to fly there,<sup>124</sup> and twelve out of thirteen 'muscle hijackers' were from Saudi Arabia,<sup>125</sup> highlighting the international reach of the planning prior to 9/11. Assistance for training and travel were also said to have come from Hezbollah, based in Lebanon, and Iran.<sup>126</sup> Furthermore, the financing itself came from a wide variety of sources, including through a network of donors in the Gulf States,<sup>127</sup> particularly those based in Saudi Arabia.<sup>128</sup> The 9/11 Commission Report claimed this was mainly channelled through hawala, an informal value transfer system based on trust which, at the time, could be transferred internationally and without incriminating paper records.<sup>129</sup> Furthermore, the hijackers were wired a total of \$114,500 sent in five transfers between \$5,000 and \$70,000 from Dubai by Khalid Sheik Mohammed's nephew, Ali Abdul Aziz, who himself remarked

---

<sup>121</sup> *9-11 Commission Report* <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016, 160-165.

<sup>122</sup> *ibid.*

<sup>123</sup> *ibid* 169.

<sup>124</sup> *ibid* 225-226.

<sup>125</sup> *ibid* 231-232.

<sup>126</sup> *ibid* 240-241.

<sup>127</sup> *ibid* 170.

<sup>128</sup> *ibid.*

<sup>129</sup> *ibid* 172.

that his transactions were essentially invisible due to the billions of dollars flowing daily on a global level.<sup>130</sup> The hijackers also opened bank accounts once they arrived in the US.<sup>131</sup> Finally, the communications the hijackers also used in the run up to the World Trade Center attacks were through coded email – with Mohamed Atta sending the other hijackers the message, referring to the targets, that *‘the semester begins in three more weeks. We’ve received 19 confirmations for the faculty of law, the faculty of urban planning, the faculty of fine arts and the faculty of engineering...’*<sup>132</sup> This awareness of masking planning, communications and financing through global systems is even more relevant 15 years later, with Islamic State using the next generation of global communications and financial systems - social media, the Dark Web and digital currency, in order to secretly further their aims, fund their activities and gather recruits to their Syrian strongholds from as far away as the US and Australia.<sup>133</sup> It is therefore imperative that any methodology used to study the financing of terrorism has a comparative and international outlook.

#### **2.4. General Research Questions:**

Parameters must be set, to narrow down the research area and provide a cogent argument. Counter-terrorism as a subject can be broad, using a wealth of experiences to define the effects of terrorism on a community. For example, viewing it from a psychological angle, by radicalisation or recruitment, or the harm that counter-terrorism policies have on a section of society. This is not the overall aim of the thesis; rather it

---

<sup>130</sup> *ibid* 224-225.

<sup>131</sup> *ibid* 241.

<sup>132</sup> Weimann, G. *www.terror.net – How Modern Terrorism uses the Internet* (March 2004) Special Report 116 United States Institute of Peace 10.

<sup>133</sup> 150 Australian converts travelled to Iraq and Syria by 2015; Wilson, L. (News.com.au., 28 March 2015) *The rapid evolution of the ISIS death cult* <<http://www.news.com.au/world/middle-east/the-rapid-evolution-of-the-isis-death-cult/news-story/74f78cd251d7d700cfb9645c5b119f3d>> accessed 16 October 2016.

examines these points from the narrower angle of financial crime. The overarching questions leading this thesis are therefore as follows:

- Has the ‘Financial War on Terrorism’ worked since 9/11?
- Can CTF/anti-money laundering (AML) legislation after 9/11 be transposed effectively onto Internet communications and transactions?
- Have countries exceeded or fallen short of international standards on human rights and financial crime?
- What preventative solutions can be made through comparing individual countries’ measures against financial crime and Internet usage?

On looking at the subsequent academic and Government studies to the events of 9/11, it is clear that they have centred on the recruitment techniques of terrorist organisations and radicalisation, or, when looking at financial crime, just one of two key elements of counter-terrorist financing and Internet communications – the ‘traditional forms’ of raising and channelling finances (for example, through criminal activities such as smuggling and through formal financial institutions) and using the Internet as a propaganda tool for recruiting new converts. Even Todd Hinnen, the former Acting Assistant Attorney General for National Security in the US Department of Justice, whose seminal research into terrorist financing and the Internet in 2004 forms the basis of this thesis, included using the Internet as a form of propaganda to target new recruits,<sup>134</sup> essentially diluting the powerful notion that the Internet is being used to raise and channel much-needed finances to terrorist organisations. By comparison, within this thesis, any mention of, for example, radicalisation, will be in direct connection with the rising problem of ‘cheap terrorism’, where nominal amounts of

---

<sup>134</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5.

cash are raised and channelled through financial systems, meaning that authorities have to look for a different way of preventing terrorist acts.<sup>135</sup> Any argument which does not solely focus on terrorist financing risks it being part of a wider problem, which detracts from former President Bush's proclamation to '*follow the money*' when tracing and disrupting terrorist organisations.<sup>136</sup> Financing is an essential part of terrorism and, fifteen years on from 9/11, we are now at the stage where Internet banking and using digital currency are parts of everyday life. Therefore, one of the main questions is how international organisations and national governments can prevent the proliferation of terrorist financing through rapidly emerging Internet transactions and communications.

Furthermore, 9/11 and the resulting 'Financial War on Terror' were watershed moments in the fields of both counter-terrorism and financial crime. The first question is therefore why the US and other countries failed to find out such a highly co-ordinated attack was being planned. By charting and comparing the background histories of selected countries and the UN, it is key to finding out why important moments in the run up to 9/11 were missed and whether such mistakes have been repeated again

---

<sup>135</sup> For example, the 7/7 bombings cost £8,000 – well below the trigger for a Suspicious Activity Report of £10,000 – Harrison K. & Ryder N. *The Law Relating to Financial Crime in the United Kingdom* (2<sup>nd</sup> Edn. Routledge, 2016), 43; With Madrid, it is estimated that it cost \$10,000 to carry out the attacks, which consisted of thirteen bombs and killed 191 people during the morning rush hour on 11 March 2004 – United Nations Security Council S/2004/679 *First report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities* (25 August 2004), 12 <<http://www.un.org/docs/sc/committees/1267/1267mg.htm>> accessed November 2016; after the Boston bombings on 15 April 2013, it was found that Dzhokhar and Tamerlan Tsarnaev used pressure cookers and cheap, low grade explosives to carry out their acts, killing three people and injuring 264 – *United States v. Dzhokhar A. Tsarnaev* (District Court of Massachusetts, Case Number: 1:13-cr-10200) [24], [25], 8, <<http://www.justice.gov/usao/ma/news/2013/April/criminalcomplaint1304211847.pdf>> accessed November 2016.

<sup>136</sup> "*We will starve terrorists of funding, turn them one against another, drive them from place to place until there is no refuge or no rest...*" President George W. Bush *Joint Session of Congress Concerning the September 11, 2001 Terrorist Attacks on America* Congressional Record Volume 147, S9553-S9555 (GPO, 20 September 2001) <<http://www.gpo.gov/fdsys/pkg/CREC-2001-09-20/pdf/CREC-2001-09-20-pt1-PgS9553-4.pdf#page=1>> accessed November 2016.

– eventually leading to conclusions and recommendations on prevention. Additionally, since the Bali Bomber’s ‘Manifesto’ in 2002,<sup>137</sup> in which he highlighted ways to commit cybercrime in order to fund terrorist acts,<sup>138</sup> the subsequent question should be how countries involved in the War on Terror responded to the twin issues of counter-terrorist financing and Internet communications and whether they have been effective enough to prevent future acts of terror on the same scale.

Finally, there are two overarching questions which run through the thesis itself – through blackletter law, secondary legislation, Government policy and caselaw – whether the measures since 9/11 have been effective and appropriate. Striking a balance between the need to find potential transactions relating to terrorist organisations or acts, and the international human right of privacy is an important part of this research. It is an accepted anathematic principle to suggest that the majority of Internet users, who use the Internet for perfectly legal and everyday purposes, should be subject to overly intrusive surveillance techniques which, although being exceptionally effective in tracing terrorist financing, could debase their ordinary rights.

## **2.5. The selection of key examples:**

To select specific examples of CTF, as well as Internet communications, first it is necessary to ensure that the thesis is focused on countries which have the capability of openly publishing their data, or have been assessed by international organisations such as the Financial Action Task Force (FATF), which has peer-to-peer assessments of Members’ and Observers’ AML and CTF provisions,<sup>139</sup> in order to create a complete comparison. Second, on using Hinnen’s three ways of raising and channelling

---

<sup>137</sup> Goodman, M. *Future Crimes* (1st Edn. Transworld Publishers, 2015), 51.

<sup>138</sup> *ibid.*

<sup>139</sup> See in general <[www.fatf-gafi.org](http://www.fatf-gafi.org)> accessed November 2016.

financing through the Internet as a basis,<sup>140</sup> there must also be clear comparisons between each country on their policies regarding Internet surveillance as well as the ability to analyse whether they are appropriate and effective. Third, there must be an evident telecommunications structure, whether state-owned or not, to show that those residing or using telecommunications in that country have the capability to transfer or raise funds through the Internet and are subject to monitoring requirements. Finally, those countries with direct experience of terrorist acts would automatically have subsequent legislation which would attempt to prevent future terrorist acts, providing a comparison and enabling the author to find best or worst practice examples. For example, using Timor Leste, which has low Internet penetration rates<sup>141</sup> and a low threat of terrorism,<sup>142</sup> as a country to compare would be counter-productive, as it would not provide a clear comparison to other countries which have focused on preventing and disrupting terrorist financing, such as the US. Additionally, using only Westernised countries, such as the US, UK, Canada and Australia, would not provide the breadth and depth of data required to ensure a fully rounded argument.

### **2.5.1. The United States:**

The US is an important country to analyse in this context. Not only was it the ‘victim’ of 9/11,<sup>143</sup> as this was the pinnacle of repeated al-Qaeda attacks on US citizens,<sup>144</sup> but

---

<sup>140</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5.

<sup>141</sup> Groden, C. M. *These Countries Have the World's Worst Internet Access* (Fortune.com, 6 October 2015) <<http://fortune.com/2015/10/06/worst-internet-access/>> accessed 15 October 2016.

<sup>142</sup> UK Government Foreign Office Travel Advice *Timor Leste* <[www.gov.uk/foreign-travel-advice/timor-leste](http://www.gov.uk/foreign-travel-advice/timor-leste)> accessed 15 October 2016.

<sup>143</sup> In co-ordinated attacks, 9/11 caused the deaths of nearly 3,000 people on US soil; *9-11 Commission Report* (22 July 2004) <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016>, Chapter 9 (fn.188).

<sup>144</sup> For example, co-ordinated attacks by al-Qaeda on US Embassies in Kenya and Tanzania in 1998 – Federal Bureau of Investigation ‘*East African Embassy Bombings*’ <<https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings>> accessed November 2016.

it declared the ‘War on Terror’,<sup>145</sup> stating that the “*terrorist attacks of September 11, 2001, in Washington, D.C., New York City, and Pennsylvania were acts of war against the United States of America and its allies*”.<sup>146</sup> President George W. Bush also declared a ‘Financial War on Terrorism’ on 24<sup>th</sup> September 2001, freezing the assets of 27 entities suspected of terrorist financing,<sup>147</sup> bringing this matter to international attention<sup>148</sup> and, ultimately, bringing it before the attention of the United Nations Security Council. As Ryder states, the Financial War on Terror “*was a direct reaction to the financing of terrorism, which was previously neglected by the international community*”,<sup>149</sup> a point confirmed by the fact that there were only four signatories to the 1999 UN Convention on the Suppression of the Financing of Terrorism prior to 9/11.<sup>150</sup> The influence of the US on the UN Security Council is also not to be underestimated, as the Council issued a binding Resolution on all 193 UN Member States regarding counter-terrorist financing just days after the attacks.<sup>151</sup> It should be noted

---

<sup>145</sup> President George W. Bush *Joint Session of Congress Concerning the September 11, 2001 Terrorist Attacks on America* Congressional Record Volume 147, S9553-S9555 (GPO, 20 September 2001) <<http://www.gpo.gov/fdsys/pkg/CREC-2001-09-20/pdf/CREC-2001-09-20-pt1-PgS9553-4.pdf#page=1>> accessed November 2016.

<sup>146</sup> United States *National Strategy for Combating Terrorism* (14 February 2003), 1 <[https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter\\_Terrorism\\_Strategy.pdf](https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf)> accessed June 2018.

<sup>147</sup> The Whitehouse Archives *President Freezes Terrorists’ Assets* (24 September 2001) <<https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>> accessed November 2016.

<sup>148</sup> *ibid* President George W. Bush, *Joint Session of Congress Concerning the September 11, 2001 Terrorist Attacks on America; National Strategy for Combating Terrorism*, 17-19 <[https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter\\_Terrorism\\_Strategy.pdf](https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf)> accessed June 2018.

<sup>149</sup> Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001*. (Routledge, 2015), 2.

<sup>150</sup> *ibid* 6.

<sup>151</sup> UN Security Council Resolutions S/RES/1368 Counter-Terrorism Implementation Task Force (12 September 2001) and S/RES/1373 Threats to international peace and security caused by terrorist acts (28 September 2001).



that the US is a permanent member of the UN Security Council,<sup>152</sup> and two other members are also members of the defensive North Atlantic Treaty Organisation,<sup>153</sup> for which the US provides nearly a quarter of the shared funding.<sup>154</sup> It is also worthy to observe that, at the time of the 9/11 attacks, the UN Security Council Presidency was held by France<sup>155</sup> which has been an ally of the US since 1778.<sup>156</sup> Additionally, the US is a founding member of the FATF,<sup>157</sup> an international body tasked with monitoring international CTF and AML through a series of Recommendations and peer-to-peer reviews, for example, under the 1999 Convention and UN Resolution 1373.<sup>158</sup> Consequently, these influences have been leveraged to ensure other Member States were bound to apply counter-terrorist financing provisions as set out in the 1999 UN Convention.

Further supporting the use of the US as an example, is the point that the US has been a world leader in combating financial crime, with its experience being long and varied.<sup>159</sup> Since the Racketeer Influenced and Corrupt Organizations Act of

---

<sup>152</sup> There are only five permanent members of the Security Council – the US, the UK, Russia, China and France, UN Security Council website <<http://www.un.org/en/sc/members/>> accessed November 2016.

<sup>153</sup> The United Kingdom and France – overall, there are 28 members of NATO; NATO website <[http://www.nato.int/cps/en/natohq/nato\\_countries.htm](http://www.nato.int/cps/en/natohq/nato_countries.htm)> accessed November 2016.

<sup>154</sup> It contributes approximately 22% of the shared funding budget. Whitehouse Press Office *FACT SHEET: U.S. Contributions to NATO Capabilities* (8 July 2016) <<https://www.whitehouse.gov/the-press-office/2016/07/08/fact-sheet-us-contributions-nato-capabilities>> accessed November 2016.

<sup>155</sup> United Nations Security Council *SECURITY COUNCIL CONDEMNS, 'IN STRONGEST TERMS', TERRORIST ATTACKS ON UNITED STATES* (12 September 2001) <<https://www.un.org/press/en/2001/SC7143.doc.htm>> accessed November 2016, which mentions the President, Jean-David Levitte (France) as the President of the Security Council at the time.

<sup>156</sup> France was the first ally of the United States during the War of Independence in 1778. US Department of State *The Treaty of Alliance with France; US Department of State U.S. Relations with France* (21 July 2016) <<http://www.state.gov/r/pa/ei/bgn/3842.htm>> accessed November 2016.

<sup>157</sup> This is through the G7 or the 'Group of 7' nations. The United Kingdom and United States are founding members of the Financial Action Task Force <[http://www.fatf-gafi.org/document/52/0,3343,en\\_32250379\\_32236869\\_34027188\\_1\\_1\\_1\\_1,00.html](http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32236869_34027188_1_1_1_1,00.html)> accessed November 2016.

<sup>158</sup> FATF Recommendation 6.

<sup>159</sup> *ibid* Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Routledge, 2015), 6.

1970,<sup>160</sup> which first dealt with illicit profits from Mafia organisations being re-invested into the US economy, with seminal financial weapons, including the forfeiture of assets,<sup>161</sup> and the Bank Secrecy Act of 1970 which first introduced currency transaction reports,<sup>162</sup> the US has been at the forefront of preventing and detecting this type of crime and, in particular, AML. Furthermore, regarding CTF, it was noted that the US was a ‘heavy’ influence behind the 1999 UN Convention was the al-Qaeda attack on US embassies in Kenya and Tanzania.<sup>163</sup> Using the US as a basis to compare each example, as well as the overarching international regulations, is therefore paramount as part of this thesis.

The US is also home to a number of Internet Service Providers, which physically run their fibre-optic cables from the US worldwide,<sup>164</sup> and is also the centre for Internet Corporation for Assigned Names and Numbers (ICANN) – the Internet Domain Name registration service responsible for websites worldwide. The involvement of the US on these levels is significant; it has the potential to access and subvert information which may be outside of its constitutional and international restraints (for example, accessing SWIFT to gain information about European bank accounts).<sup>165</sup> Furthermore, it has been at the forefront of some of the most controversial Internet surveillance techniques in the world since 9/11, including email surveillance measures

---

<sup>160</sup> §1962(a) Chapter 96, Title 18, United States Code.

<sup>161</sup> §1963(a), (b) and (c), Chapter 96, Title 18 U.S.C.

<sup>162</sup> The Financial Recordkeeping and Currency and Transactions Reporting Act of 1970 (“Bank Secrecy Act”) (Pub. L. 91-508, 84 Stat. 1118) 31 U.S.C. §5311

<sup>163</sup> *ibid* Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Routledge, 2015), 6.

<sup>164</sup> For example, to Europe through the UK’s Transatlantic Fibre Optic Cables- this came to a head during Edward Snowden’s allegations of GCHQ and the NSA procuring information from the fibre optic cables through the PRISM programme. See Chapters Four and Five for further information.

<sup>165</sup> European Parliament *MEPs call for suspension of EU-US bank data deal in response to NSA snooping* (23 October 2013) <http://www.europarl.europa.eu/news/en/press-room/20131021IPR22725/meps-call-for-suspension-of-eu-us-bank-data-deal-in-response-to-nsa-snooping> accessed June 2018.

under Title II of the USA PATRIOT Act of 2001,<sup>166</sup> mass surveillance and secretive courts under the Foreign Intelligence Surveillance Act of 2008<sup>167</sup> and working in partnership with the UK's GCHQ to gather information about Internet users under the PRISM Programme.<sup>168</sup> Consequently, all of these measures have significant impacts on other countries' use and monitoring of the Internet. Finally, its constitutional similarities and relationship with the UK are important; both have been leaders of international action against terrorism and there are aspects of similarity and comparisons to make between their conduct since 9/11.

### **2.5.2. The United Kingdom:**

The UK is a significant comparative point. First of all, it does not have a written constitution,<sup>169</sup> enabling its courts to derive decisions on the common law principle of precedent,<sup>170</sup> and allowing a more flexible and potentially wider interpretation of counter-terrorism law. Second, the UK is, at present, part of the EU, which highlights a regional aspect to its CTF – and that it is subservient to EU law and judgements in this area, which creates a conflict between a Napoleonic set of Codes which and its own historical common law.<sup>171</sup> Third, the UK has significant gaps in its own law –

---

<sup>166</sup> Chapter four, 4.1.2.

<sup>167</sup> Chapter four, 4.1.2.

<sup>168</sup> Chapters four, 4.1.2. and five, 5.1.2.a. and b.

<sup>169</sup> Blackburn, R. *Magna Carta* (British Library) <<https://www.bl.uk/magna-carta/articles/britains-unwritten-constitution>> accessed November 2016.

<sup>170</sup> Also known as *stare decisis*, including the *ratio decidendi* and *obiter dictum* of cases.

<sup>171</sup> For example, the four Anti-Money Laundering Directives (Directives 91/308/EEC, 2001/97/EC, 2005/60/EC and 2015/849/EU) preside over counter-terrorist financing - although they provide guidance to Member States rather than binding rules – have an impact on the UK's provisions against money laundering and terrorist financing. The Lisbon Treaty - 2007/C 306/01 changed the 'pillar' structure of European Union legislation, meaning that criminal matters will be dealt with in the same manner as single market legislation.

such as lacking the ability to use intercept evidence in court evidence – which the US has as part of its justice system.<sup>172</sup> These together provide good comparative points.

Most importantly, however, the UK was subject to terrorist acts over a century before 9/11, creating specific and separate laws to combat terrorist financing. For example, this included the Northern Ireland (Emergency Provisions) Act 1973, the Prevention of Terrorism (Temporary Provisions) Act 1974 and the Prevention of Terrorism (Amendment) Act 1989. These laws predate both UN and US action on CTF – as the US and the UN during the 1980s concentrated on money laundering through drugs offences, most significantly through the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1988,<sup>173</sup> which criminalised money laundering in the event of drug trafficking.<sup>174</sup> Instead, the UK, and subsequently the EU, widened the offence of money laundering to include predicate offences such as terrorist financing.<sup>175</sup> Clearly, this separation of terrorist financing and money laundering offences is a significant one. Unlike the US' combination of the money laundering and terrorist financing offences within the USA PATRIOT Act of 2001, the

---

<sup>172</sup> For example, the Telegraph Acts of 1863 c. 112 (Regnal. 26 and 27 Vict) and 1868 c. 110 (Regnal. 31 and 32 Vict) prohibited interception and disclosure of telegraph messages by employees (s45 of the 1863 Act introduced fines and s20 of the 1868 Act introduced a criminal offence). Furthermore, the Birkett Report of 1957 highlighted that it had been “settled policy” of the Home Office not to use intercept evidence “*save in the most exceptional cases.*” *Privy Council Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* Cmnd 283 [92] (HMSO, 1957) <<http://www.fipr.org/rip/Birkett.htm>> accessed November 2016. By comparison, at a federal level, intercept evidence can be routinely disclosed under testimony in criminal cases – see Title III Omnibus Crime Control and Safe Streets Act of 1968 (Pub.L. 90–351, 82 Stat. 197) 18 U.S.C. §2517(3). Furthermore, §203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Pub. L. 107-56, 115 Stat. 272) enhances existing disclosure rules and applies them to criminal cases involving terrorism.

<sup>173</sup> UN Treaty Series vol. 1582 No. 27627 Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (‘Vienna Convention’), Article 3(i)(b).

<sup>174</sup> The Convention specifically states that criminalisation is in specific connection with drugs trafficking under Article 3(a).

<sup>175</sup> Part VI Criminal Justice Act 1988, c. 33; Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering (‘First Money Laundering Directive’). See Chapter Three at 3.1.3.

UK's understanding that this is a separate offence to money laundering, and using investigatory powers to focus on what is essentially a different financial crime<sup>176</sup> is important in finding a way forward for financial crime after 9/11.

### **2.5.3. Kingdom of Saudi Arabia:**

The relationship between the US, UK and Saudi Arabia is sometimes fragile, yet is continued despite allegations that a number of 9/11 donors were based there.<sup>177</sup> As a Gulf State which is open to analysis by the FATF,<sup>178</sup> Saudi Arabia was subject to a terrorist attack in Riyadh in 2003<sup>179</sup> and, along with involvement in the Syrian conflict against Islamic State,<sup>180</sup> it is clear that the intentions of Saudi Arabia are to prevent terrorist financing within the confines of international law. Furthermore, Saudi Arabia is confined to Shari'ah law,<sup>181</sup> raising the question that, although it is bound by international law on counter-terrorist financing, whether it can apply these sufficiently

---

<sup>176</sup> In comparison with the US, the UK has a broader and more detailed definition of terrorism and what constitutes a terrorist act under the Terrorism Act 2000 c.11 (e.g. it includes disruption of electronic systems under s1(2)(e)). Significantly, the definition of terrorism under s1 of the Terrorism Act 2000 c.11 expressly includes the "threat of action". This is different to the definition in U.S.C. Title 22, Ch.38, Paragraph 2656f(d), which does not include this wording. Interestingly, Lord Lloyd of Berwick, in his *Inquiry Into Legislation Against Terrorism* in 1996, suggested that the definition of terrorism should be based upon the operational definition used by the FBI during the 1990s – see Lord Lloyd of Berwick *Inquiry into Legislation Against Terrorism* Volume 1 Cm 3420 (HMSO, 1996); Lord Carlile of Berriew *The Definition of Terrorism* Cm 7052 (Home Office, March 2007), 3 para. 9 <<https://www.gov.uk/government/publications/the-definition-of-terrorism-a-report-by-lord-carlile-of-berriew>> accessed April 2018.

<sup>177</sup> 9-11 Commission Report (22 July 2004) <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016>, 170.

<sup>178</sup> Middle East North Africa Financial Action Task Force <<http://www.menafatf.org/>> accessed November 2016.

<sup>179</sup> CNN (9 November 2003) *Saudi official blames Riyadh attacks on al Qaeda* <<http://edition.cnn.com/2003/US/11/08/saudi.explosion/>> accessed November 2016.

<sup>180</sup> BBC News (3 December 2015) *Islamic State: Where key countries stand* <<http://www.bbc.co.uk/news/world-middle-east-29074514>> accessed November 2016.

<sup>181</sup> MENAFATF *Mutual Evaluation Report on Saudi Arabia* (25 June 2010) 15, para. 53; 16, para. 54 <[www.fatf-gafi.org](http://www.fatf-gafi.org)> accessed November 2016; Basic Law of 1992 Article 8.

NB. Criminal conduct relating to financial crime should be viewed in the same light as Western countries because Saudi Arabia is signatory to a number of UN Conventions on this issue, e.g. Vienna and Palermo Conventions; NB. Shari'ah is based on five principles laid down in Islamic holy texts

through its current legal system. Additionally, Saudi Arabia, despite its links with the US and the UK, is a notoriously repressive country, controlling its Internet communications through a Government department,<sup>182</sup> and punishing dissent from Internet bloggers.<sup>183</sup> Consequently, Saudi Arabia is an important aspect of comparison, when assessing whether some countries, such as the UK, are moving further away from accepted privacy norms in terms of their surveillance techniques.

## 2.6. Literature Review:

Literature reviews have often been described as “*provid[ing] us with a theoretical framework for our research, as well as a justification for carrying it out.*”<sup>184</sup> Consequently, it is imperative that the literature review highlights not only the context of the thesis, but also gaps in thought and research. Bryman notes that the existing literature should be explored to identify the following:<sup>185</sup>

- ☐ *What is already known about this area?*
- ☐ *What concepts and theories are relevant to this area?*

---

regarding human acts – obligatory (*wajib*), recommended (*mandub*), permissible (*mubah*), reprehensible (*makruh*) and forbidden (*haram*). Legal qualities are found in two principle sources – the Qur’an, and the *sunnah*, or the oral traditions regarding the words and deeds of the Prophet Mohammed. Furthermore, there is the doctrine of *ijma*, or consensus, which means that any legal decision which has been agreed upon unanimously, at any time, is the correct conclusion, as well as *qiyas*, the analogical reasoning and determination of the legality of certain acts, even when they are not clearly defined in the Qur’an or the *sunnah*. Lombardi, C.B. *Islamic Law as a Source of Constitutional Law in Egypt: The Constitutionalization of the Sharia in Modern Arab States* (1998) 37(1) Columbia Journal of Transnational Law 81 – although this refers to Egypt specifically, this text provides a clear overview of Shari’ah law.

<sup>182</sup> King Abdulaziz City Science and Technology Unit set up in 1998 <<http://www.kacst.edu.sa/en/services/Pages/internetservices.aspx>> accessed November 2016; now undertaken by the Communications and Information Technology Commission as an implementation of the Council of Ministers Resolution No. 229 date 13.08.1425 H Communications and Information Technology Commission *About Us* <<http://www.citc.gov.sa/en/AboutUs/Pages/History.aspx>> accessed April 2018.

<sup>183</sup> For example. Raif Badawi, who was sentenced to 1,000 lashes for exercising his freedom of speech, Amnesty International *Raif Badawi* <<https://www.amnesty.org.uk/issues/Raif-Badawi>> accessed November 2016.

<sup>184</sup> Henn et al. *A Short Introduction to Social Research* (2006, SAGE Publications), 227.

<sup>185</sup> Bryman, A. *Social Research Methods* (2nd Edn. Oxford University Press, 2004), 526.

- ☐ *What research methods and research strategies have been employed in studying this area?*
- ☐ *Are there any significant controversies?*
- ☐ *Are there any inconsistencies in findings relating to this area?*
- ☐ *Are there any unanswered research questions in this area?*

With these questions in mind, the literature review should also show how the arguments and results in this thesis differs from other scholars in the field of research, highlighting its significant contribution to research. The literature review of this thesis is therefore split into two main themes, given that it focuses on CTF and Internet regulation.

### **2.6.1. Counter-Terrorist Financing after 9/11**

Since 9/11, there has been a wealth of sources and academic analysis surrounding CTF. Yet, over the course of a decade, these tended to focus on more ‘traditional’ forms of CTF, i.e. state sponsorship of terrorism, using the formal banking system, Informal Value Transfer Systems such as *hawala*,<sup>186</sup> charities as a ‘front’ and gathering illicit finances through smuggling drugs. For example, prolific academics and commentators in this area, such as Ryder<sup>187</sup> and Gurulé,<sup>188</sup> had written about these

---

<sup>186</sup> Ryder N. *Financial Crime in the 21<sup>st</sup> Century: Law and Policy* (Edward Elgar, 2011), 54.

<sup>187</sup> For example, see Ryder N. *The Financial War on Terror: A review of counter-terrorist financing strategies since 2001* (Routledge, 2015), 210; *Out with the old and ... in with the old? A critical review of the Financial War on Terrorism on the Islamic State of Iraq and Levant* (2016) *Studies in Conflict and Terrorism* (Special issue on ‘Contemporary Issues, Innovation and Counter Terrorism’), accepted for publication. *Banks in Defense of the Homeland: Nexus of Ethics and Suspicious Activity Reporting* (2013) *Contemporary Issues in Law* (Special Issue on Law, Ethics and Counter-Terrorism), 12(4), 311-347; with Türkşen, U *Islamophobia or an important weapon? An analysis of the US financial war on terrorism*, (2009) *Journal of Banking Regulation* 10(4) 307-320; *A false sense of security? An analysis of legislative approaches to the prevention of terrorist finance in the United States of America and the United Kingdom*, (2007) *Journal of Business Law*, November, 821-850.

<sup>188</sup> NB. Gurulé was head of anti-terrorist financing in the US Treasury between 2001 and 2003.

topics extensively at the time,<sup>189</sup> but had not yet broached the area of Internet transactions and the abuse of the Internet by terrorist financiers. Indeed, few academics had written about this without referring to it as part of the traditional forms of financing terror. However, as far back as 2005, academics such as Baldwin had examined the Internet by terrorist financiers-<sup>190</sup> although, on reading his work, there is a sense that this is ‘stuck’ in its time, due to his focus on the online marketplace, and not the forms of electronic transaction which were emerging at the time.<sup>191</sup> Furthermore, Hinnen, whose work this thesis is based upon, carried out his research in 2004, using terrorist financing to form part of a larger work on terrorist use of the Internet.<sup>192</sup> It has only been relatively recently, within the last five years or so, that more academics and policy-makers have realised that the use of the Internet is pervasive in everyday life, and that this normalisation has enabled terrorists to use it as part of their network of financing. Yet, again, on looking at the academic output, this fails to purely examine terrorist financing via the Internet – it is always used as part of the overall argument on terrorist use of the Internet.<sup>193</sup> Therefore, the literature used, although some based on traditional forms of CTF and others based on the use of the internet by terrorists, must be weighed carefully against the overall arguments within the thesis. Each comment and analysis in this area has merit, and can be used, moderately, to identify both the surrounding doctrine in this subject, and the gaps in knowledge to create a significant piece of work. Here, the differences between existing academic work and this

---

<sup>189</sup> E.g. Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008); Gurulé, J. & Corn, G.S. *Principles of Counter-Terrorism Law* (1<sup>st</sup> Edn. Thompson-West, 2011).

<sup>190</sup> Baldwin, F.N. *The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?* (2004) 8(2) *Journal of Money Laundering Control* 127, 157 – 158.

<sup>191</sup> *ibid* 134-136.

<sup>192</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5; also see 2.4 of this chapter.

<sup>193</sup> For example, see Keene, S.D. *Terrorism and the internet: a double-edged sword* (2011) *Journal of Money Laundering Control*, Vol. 14 Iss 4, 359 – 370– again, CTF is used as a part of a broader argument.



thesis are clear – no academic work that has been found uses Saudi Arabia as an example to compare with other countries. It is often cited as a ‘standalone’ country, and little has been written about how it fits into the model of international law on counter-terrorist financing. Furthermore, despite the rise of the Islamic State of Iraq and the Levant (ISIL) and its slick use of business models and annual reports in *al Naba* to carry out its aims,<sup>194</sup> the existing work on this area focuses on al-Qaeda and becomes quickly outdated once the methods they use to raise and channel finances are taken into account. By focusing on current threats and providing Saudi Arabia as a comparator, this thesis will form a significant contribution to knowledge.

#### **2.6.2. Internet filtration and surveillance in the modern age**

This is, perhaps, the most diversified area within the thesis, as theories and research on Internet surveillance is incredibly wide and varied. In order to narrow the scope of data surveillance and the resulting use of certain pieces of legislation and commentary, as well as making it relevant to CTF, it is first necessary to have a fixed starting point. Therefore, Hinnen’s outline of terrorist financing and the Internet has been used to apply data surveillance measures in the limited context of direct solicitation of donations (broken down into websites and email communications), use of legitimate institutions (broken down into formal financial institutions and charities) and online crime (separated through cyber-laundering and online fraud). By carrying out this limitation, the author can substantially examine surrounding legislation and commentary sufficiently, to provide an overall picture of international measures pertaining to CTF and

---

<sup>194</sup> Khalaf, R. & Jones, S. (Financial Times, 17 June 2014) *Selling terror: how Isis details its brutality* <<https://www.ft.com/content/69e70954-f639-11e3-a038-00144feabdc0>> accessed November 2016; Malik, S. (The Guardian, 7 December 2015) *The Isis papers: leaked documents show how Isis is building its state* <<https://www.theguardian.com/world/2015/dec/07/leaked-isis-document-reveals-plan-building-state-syria>> accessed November 2016.

the Internet. It is clear from the research undertaken that a great number of commentary pieces about Internet surveillance are written from the angle of potential national and international human rights abuses – which, although answering the question of appropriateness, does not provide a balanced argument when dealing with effectiveness. For example, while Lodgson argues that much of the US’ data surveillance programmes have violated the Constitution’s Fourth Amendment,<sup>195</sup> it is necessary to have a counter-argument through analysing effectiveness – as they have proved incredibly successful because of convictions such as *United States v Jamie Paulin Ramirez*<sup>196</sup> and *United States v Colleen LaRose*,<sup>197</sup> which prevented a potential terrorist attack. Furthermore, on examining literature based on counter terrorism and surveillance, such as Donohue,<sup>198</sup> there is a sense that, if at all, a comparative piece of work is only based on two jurisdictions and, perhaps, the United Nations. Some of the commentary and analysis about Internet surveillance and website filtration also concentrates on one country only.<sup>199</sup> This is a substantial gap in knowledge and limits seeking solutions to, what is, an immediate global danger. The lack of a UN Convention or UN Security Council Resolution on data surveillance and Internet monitoring makes this area complex and contradictory in places; meaning that much of this research must also rely on the UN’s Universal Declaration of Human Rights – drafted over forty years before the birth of the Internet. Resultantly, using three countries as an example provides more of an evidence base on the interpretation of CTF and use

---

<sup>195</sup> Lodgson, K.R. *Who knows you are reading this? The United States’ domestic electronic surveillance in a post-9/11 world* (2008) *Journal of Law Technology & Policy* 409, 420.

<sup>196</sup> *United States v. Jamie Paulin Ramirez* Eastern District of Pennsylvania 8 March 2011.

<sup>197</sup> *United States v. Colleen LaRose* E.D. Pa 1 February 2011.

<sup>198</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008); Donohue, L.K. *Anti-Terrorist Finance in the United Kingdom and United States*, 27 *Mich. J. Int’l L.* 303-435 (2006).

<sup>199</sup> E.g. Ferguson, G. & Wadham, J. *Privacy and Surveillance: A review of the Regulation of Investigatory Powers Act 2000* (2003) *European Human Rights Law Review* 101.

of data surveillance measures, providing the author with an opportunity to seek solutions and recommendations in this highly controversial and still developing area of law. As noted earlier, the rise of ISIL has been an important factor, both through their forms of raising finances as well as their use of the Internet to further their aims and groom recruits to join them in Syria and Iraq.<sup>200</sup> Therefore, this marks the thesis apart from existing academic work in this area. Through comparing surveillance and monitoring since the rise of ISIL, there is more of an understanding why they need to be effective and, perhaps, why there is more intrusion on the private lives of many users of the Internet.

### **2.6.3. Overall Data Collection Techniques**

To analyse and compare countries sufficiently, data collection must take a variety of forms. Primarily, the legislation and policy of each country has to be analysed at source, to provide a clear doctrinal and qualitative guide to the principles they adhere to. For instance, the UK's Investigatory Powers Bill, must be analysed as amendments are produced and criticisms of its proposals are outlined to Members of Parliament in Committee, as it is not only a significant piece of proposed legislation, but will not receive Royal Assent until after this thesis is completed – therefore no complete academic comment is available. Second, from searching through and outlining academic analysis and caselaw, this creates a picture of how this legislation has been interpreted by peers and both international and national courts, as well as whether it is seen as appropriate or effective within the context of counter-terrorist financing. By analysing secondary sources such as these, questions and recommendations can also be raised,

---

<sup>200</sup> The Telegraph *How terrorists are using social media* (4 November 2014) <<http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html>> accessed November 2016.

allowing the author to provide relevant conclusions about the effectiveness and appropriateness of each regulation. However, the author notes that such content must be rigorously accounted for – as, for example, Jean-Charles Brisard, who provided a report to the UN alleging that senior Royals in Saudi Arabia had connections to the 9/11 hijacks, was subsequently successfully sued for his comments.<sup>201</sup> Furthermore, the author admits that they have used e-resources to find articles and information to support the overall argument. As Bryman notes, this “*can be regarded as potential fodder for both quantitative and qualitative content analysis*”.<sup>202</sup> Nevertheless, as Bryman further notes, “*the crucial issue is to be sensitive to the limitations of the use of web-sites as material that can be content analysed, as well as to the opportunities they offer.*”<sup>203</sup> Therefore, not only is it imperative to look at the background of the website or an author who has posted information on it, there must also be rigorous updates on their existence or movement around the web. Finally, due to the fact that both counter-terrorism and Internet surveillance are quickly evolving areas of law, often influenced by current events, it is also necessary to ensure that relevant newspaper articles are included although, again, these must be assessed on the basis of appropriateness and accuracy, by looking at other reports on an event.

## **2.7. Conclusion**

Although there is a large amount of information and comment readily available on the twin issues of CTF and Internet surveillance, they only examine limited areas of what are broad subjects. The connection between CTF and Internet transactions remains an area which is under-researched and under-used. Many articles which use CTF provide

---

<sup>201</sup> *Mahfouz v Brisard & others* [2004] EQHC 1735 (QB).

<sup>202</sup> Bryman, A. *Social Research Methods* (2nd Edn. Oxford University Press, 2004), 467.

<sup>203</sup> *ibid* 469.

it as part of an overall argument about the ‘War on Terror’ and, of those which concentrate on purely CTF, have a concentration on traditional forms of finance – both licit and illicit. Furthermore, any suggestion of CTF in connection to Internet transactions again is used as part of an overall point about communications, propaganda and recruitment strategies through the Internet, essentially weakening the notion of terrorists’ abuse of legal transactions to finance their preparations and acts. These provide limited pieces of work which are commentary rather than substantive efforts to recommend or find solutions to an important area of law.

Because of the growing reliance on forms of payment and cash flow through the Internet, now is the time to bring this subject to the foreground. This thesis aims to rectify such gaps in knowledge and policy-making. By tying together financing – which terrorist groups rely on, in order to be able to propagate their skewed views, to recruit new members, to communicate with each other and to carry out their aims – with uses of the Internet to transact and channel resources, this becomes a significant contribution to knowledge in this area. Furthermore, through comparing several jurisdictions, there is the possibility of finding best (and worst) practices which could be used as a starting point for international intervention into the use of the Internet by terrorist groups. Even though this thesis looks at CTF and Internet surveillance from a narrow angle, its impacts are far-ranging. From the tackling of ‘cheap terrorism’ to the issues of mass surveillance, policies such as national security have been used to justify what are intrusive levels of Internet supervision in some parts of the globe. Through a comparative research method, it is essential to understand that such wide-ranging differences in doctrine are no longer effective in tackling the issue of terrorist financing through Internet transactions, and that the eventual conclusion of intervention by the UN on Internet freedoms will have to be brought to bear.

### **Chapter Three: Background to the international position on financial crime and regulation of the Internet before 9/11**

*“Fighting terrorism is like being a goalkeeper. You can make a hundred brilliant saves but the only shot that people remember is the one that gets past you.”<sup>204</sup>*

#### **3.1. Introduction**

The events of September 11<sup>th</sup>, 2001 (9/11) galvanised the international community against terrorism and focused their attention towards countering the flow of terrorist financing, to prevent such organised acts from happening again. However, to critically analyse the international reaction to 9/11 and the resulting action on counter-terrorist financing (CTF) over the Internet, it is essential to first place the problem in the context of how financial crime and misuse of the Internet for terrorist activity was tackled prior to the events of 2001. Primarily, the main financial crime – money laundering – will be outlined, on which many national and international organisations concentrated before 9/11. This will show that preventing the crime of money laundering is not the same as countering the flow of terrorist financing, and that many domestic and international agencies were unprepared for this type of financial crime. Secondly, the existing legislation and international action on the misuse of computers and the Internet will be examined, through the issue of terrorists’ employment of cyberspace through cybercrime. The chapter highlights that much of the legislation on emerging computer technology was based on physical misuse of computers and cybercrime, rather than the legal use of the Internet, for example, via online transactions with banks, which

---

<sup>204</sup> Professor Paul Wilkinson Chairman of the Centre for the Study of Terrorism and Political Violence, University of St. Andrews (The Telegraph, 1 September 1992).

terrorist organisations use as part of their financing. Finally, the arguments made under the headings “Money Laundering” and “Technology” are structured in the same way, through examining the United Nations (UN), the United States (US), the United Kingdom (UK) and Saudi Arabia. This will enable a comparison between each jurisdiction’s action on financial crime and the Internet prior to September 11, 2001.

### 3.2. **Money Laundering**

Money laundering is the process of converting assets derived from illegal sources, such as organised crime and drugs trafficking, into legal finances by channelling it through banking systems and financial institutions.<sup>205</sup> The process of money laundering is also divided into three distinct stages:

- (i) *Placement* – the primary deposit of illegal proceeds in a financial institution,
- (ii) *Layering* – the separation of proceeds from their source through financial transactions via foreign bank accounts or shell companies, and
- (iii) *Integration* – the returning of proceeds into a legal economy.<sup>206</sup>

Both terrorist financing and money laundering have the same goal, which is to conceal money,<sup>207</sup> and both use the same methods of concealing such transactions.

---

<sup>205</sup> Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 Tul. Journal Int’l & Comp. Law 161, 162.

<sup>206</sup> Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835, 842-845; *ibid* Barbot, 167-168; Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 177-179.

<sup>207</sup> Donohue, L.K. *Anti Terrorist Finance in the United States and the United Kingdom* (2005-2006) 27 Michigan Journal of International Law 303, 393.

For example, formal bank accounts, remittance services and wire transfers<sup>208</sup> as well as having the same dependence on lack of transparency and monitoring by law enforcement agencies.<sup>209</sup> However, unlike money laundering, which “*depends upon an underlying crime*”,<sup>210</sup> terrorist financing can be a mixture<sup>211</sup> of money laundering<sup>212</sup> and the conversion of *legal* finances for *illegal* purposes,<sup>213</sup> often known as reverse money laundering.<sup>214</sup> Interestingly, after 9/11, the then President, George W. Bush, considered terrorist financing as a *greater* threat than money laundering.<sup>215</sup> As a result, it is evident that money laundering and terrorist financing need separate forms of legislation to enable law enforcement authorities to trace and prevent both types of financial crime, although some critics of this approach state that problems for prosecutors occur when a defendant may be under suspicion for assisting with either offence and it is not clear which.<sup>216</sup>

Before 9/11, it was evident that the international community focused its efforts on the prevention of money laundering. Clearly, the amount generated globally from money laundering was the initial driving force behind international action<sup>217</sup> against

---

<sup>208</sup> *ibid.*

<sup>209</sup> *ibid.*

<sup>210</sup> *ibid.*

<sup>211</sup> E.g. al-Qaeda used a mixture of donations from its network and money derived from illicit sources, *9-11 Commission Report* (22 July 2004) <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016>, 171.

<sup>212</sup> Mei Leong, A. *Chasing Dirty Money: domestic and international measures against money laundering* (2007) 10(2) *Journal of Money Laundering Control* 140-156, 141.

<sup>213</sup> Shetterly, D. *Starving the terrorists of financing: How the US Treasury is fighting the war on terror* (2005-2006) 18 *Regent University Law Review* 327, 328; Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 *Arizona Journal of International and Comparative Law* 835, 835-836.

<sup>214</sup> Cassella, S.D. *Reverse Money Laundering* (2003) 7(1) *Journal of Money Laundering Control* 92, 92; *ibid* Mei Leong, A., 141.

<sup>215</sup> See in general Harrison K. & Ryder N. *The Law Relating to Financial Crime in the United Kingdom* (2<sup>nd</sup> Edn. Routledge, 2016).

<sup>216</sup> Alexander, R. *Money Laundering and Terrorist Financing: Time for a combined offence* (2009) 30(7) *Company Lawyer* 200, 201-202.

<sup>217</sup> E.g. UN Treaty Series vol. 1582 No. 27627 *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988* (‘Vienna Convention’), Article 3(i)(b) <[http://www.unodc.org/pdf/convention\\_1988\\_en.pdf](http://www.unodc.org/pdf/convention_1988_en.pdf)> accessed November 2016; Basel Committee



this type of crime, with estimates ranging from between \$500billion<sup>218</sup> to \$1trillion<sup>219</sup> per year. Furthermore, the US' "War on Drugs", instigated by President Nixon in the 1970s,<sup>220</sup> was another driving factor behind international focus on money laundering to hide the proceeds of drug trafficking.<sup>221</sup> Bachus identifies four main reasons why the UN began to examine this type of financial crime - as money laundering harms national and international economies,<sup>222</sup> it furthers criminal activity if left unchecked,<sup>223</sup> it can threaten the reputation of financial institutions and lower their competitiveness<sup>224</sup> and as it does not promote economic growth.<sup>225</sup> Additionally, money laundering is difficult to detect, with complex transactions, such as 'structuring' many small deposits to fall below banks' reporting requirements,<sup>226</sup> using friends and family

---

*Banking Regulations and Supervisory Practices Statement of Principles 1988*; G-8 Financial Action Task Force 40 Recommendations (1990); formation of Egmont Group of Financial Intelligence Units in 1995.

<sup>218</sup> Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 175.

<sup>219</sup> Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835, 840 – Bachus also cites an International Monetary Fund estimate of between \$590bn and \$1.5tn per year, 835.

<sup>220</sup> Through the Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub.L. 91–513, 84 Stat. 1236) (21 U.S.C. Ch. 13, 801 et seq.); See also President Richard Nixon *American Presidency Project* (17 June 1971) <<http://www.presidency.ucsb.edu/ws/?pid=3048>> accessed April 2018.

<sup>221</sup> *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 176-177.

<sup>222</sup> *ibid* Bachus, A.S., 840-841; also see in general International Monetary Fund *Factsheet: The IMF and the Fight Against Money Laundering and Terrorist Financing* (10 September 2010) <<http://www.imf.org/external/np/exr/facts/aml.htm>> accessed November 2016.

<sup>223</sup> *ibid* 838.

<sup>224</sup> *ibid* 839; United Nations Office on Drugs and Crime *Introduction to Money Laundering* <<http://www.unodc.org/unodc/en/money-laundering/introduction.html?ref=menuaside>> accessed November 2016.

<sup>225</sup> *ibid* 839-840.

<sup>226</sup> *ibid* 843.

to disguise the flow,<sup>227</sup> as well as using many foreign bank accounts to disguise transactions.<sup>228</sup> Furthermore, bank secrecy in some jurisdictions can create obstructions<sup>229</sup> for law enforcement authorities when investigating financial trails.<sup>230</sup> Moreover, by keeping pace with the globalisation of trade and commerce, organised crime and the financial crimes which flowed from it<sup>231</sup> became transnational in nature,<sup>232</sup> “...represent[ing] a major challenge to national law enforcement and international co-operation as national borders no longer constituted an effective barrier...”,<sup>233</sup> a point exploited by criminals.<sup>234</sup> Therefore, the need for international co-operation was

---

<sup>227</sup> *ibid* 844.

<sup>228</sup> *ibid*; Jose Franklin Jurado Rodriguez who was convicted of money laundering on a grand scale by a Luxembourg court in 1992 (“*The Franklin Jurado case*”) *United States v. Jurado-Rodriguez* 907 F. Supp. 568 (E.D.N.Y. 1995); Blum J. A., Levi, M. Naylor & R.T. Williams, P. (eds.) *Financial Secrecy, Bank Havens and Money Laundering* (1998 – submitted to the UN Office for Drug Control and Crime Prevention) 63, 63-64; Kennedy, P. *Watching the clothes go round: Combating the effects of money laundering on economic development and international trade* (2003) 12 *Current International Trade Law Journal* 140, 140.

<sup>229</sup> E.g. *United States v. Bank of Nova Scotia* 691 F.2d 1384 (11<sup>th</sup> Cir. 1982), 462 US 1119 (1983) “*Nova Scotia I and II*”; Stessens, G. *Money Laundering: A new International Law Enforcement Model* (Cambridge University Press, 2000), 326; U.S. also had problems with bank secrecy in Switzerland; *In Re. Grand Jury Subpoena: Marc Rich and Co.* A.G. 707 F.2d 663 (2d Cir. 1983); Cass Weiland, S. *Congress and the Transnational Crime Problem* (1986) 20 *International Law* 1025, 1026; *ibid* Stessens, G., 320. See also the case of Bank of Credit, Commerce and Industry (BCCI); Kerry, J. (Sen.) & Brown, H. (Sen.) *The BCCI Affair: A Report to the Committee on Foreign Relations United States Senate* 102d Congress 2d Session Senate Print 102-140 (GPO, December 1992), s.9. Also, claims of US Department of Justice and Federal Reserve refusing to co-operate with the New York District Attorney Morgenthau during his investigations into BCCI’s fraudulent and criminal activities – *ibid The BCCI Affair: A Report to the Committee on Foreign Relations United States Senate*, s. 4.

<sup>230</sup> *ibid* Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 *Arizona Journal of International and Comparative Law* 835, 845-847.

<sup>231</sup> United Nations Secretariat’s Report A/CONF.121/22/Rev.1 *Seventh United Nations Congress on the Prevention of Crime and Treatment of Offenders* (UN Department of International Economic and Social Affairs, New York, 1986), 117, para. 84 <<http://www.asc41.com/7th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/030%20ACONF.121.22.Rev.1%20Seventh%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf>> accessed November 2016, regarding the link between organised and financial crime.

<sup>232</sup> United Nations Secretariat’s Working Paper *New Dimensions of Criminality and Crime Prevention in the Context of Development: Challenges for the Future* (Presented to the 7<sup>th</sup> United Nations Congress on the Prevention of Crime and Treatment of Offenders, Milan 26 August-6 September 1985), [9(d)], 15 <<http://www.asc41.com/7th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/028%20ACONF.121.20%20New%20Dimensions%20of%20Criminality%20and%20Crime%20Prevention%20in%20the%20Context%20of%20Development.pdf>> accessed November 2016; *ibid Secretariat’s Report A/CONF.121/22/Rev.1* (1986), 2, under “Milan Plan of Action” [1], and [83], 117.

<sup>233</sup> *ibid Secretariat’s Report A/CONF.121/22/Rev.1* (1986), 114, para. 66.

<sup>234</sup> *ibid*.

highlighted to combat this type of profitable crime.<sup>235</sup> For the reasons listed above, prior to 9/11, one of the main tasks for the UN was to prevent financial crime<sup>236</sup> and, in particular, money laundering.

### **3.2.1. The United Nations and other International Organisations**

Unlike the national territories examined later, the UN is an international organisation with 192 Member States<sup>237</sup> which was established to maintain international peace and security<sup>238</sup> as well as achieving international co-operation in solving economic, cultural, humanitarian and social problems.<sup>239</sup> Furthermore, the UN has powers to impose economic sanctions on territories<sup>240</sup> and sets international standards on issues of global concern through international agreement on resolutions, recommendations and Conventions.<sup>241</sup> Consequently, the UN is a key part of international co-operation against money laundering.

Prior to 9/11, the UN centred on the prevention of drugs trafficking and associated money laundering through the introduction of the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in 1988 (“Vienna Conven-

---

<sup>235</sup> *ibid* 117, para. 83.

<sup>236</sup> *ibid* A/CONF.121/22/Rev.1, 117, para. 84 regarding link between organised and financial crime and proposed financial weapons against both.

<sup>237</sup> United Nations *UN Membership* <<http://www.un.org/en/members/index.shtml>> accessed November 2016 for more information about Member States; only Holy See and Palestine are not members of the UN. <<https://www.un.org/en/member-states/#gotoP>> accessed November 2016.

<sup>238</sup> Article 1(1) Charter of the United Nations 1945, Chapter I, <<http://www.un.org/en/documents/charter/chapter1.shtml>> accessed November 2016.

<sup>239</sup> *ibid* Charter of the United Nations 1945, Chapter I, Article 1(3).

<sup>240</sup> Charter of the United Nations, Chapter VII, Article 41.

<sup>241</sup> NB. Often through resolutions and recommendations of the UN General Assembly which has representatives of all 193 Member States, <<http://www.un.org/en/ga/about/background.shtml>> accessed November 2016.

tion”). The Vienna Convention marked the first international instrument which criminalised money laundering,<sup>242</sup> as previous “*international agreements emphasized controlling the production of drugs and preventing their flow into the market place...*”.<sup>243</sup> For example, the Single Convention on Narcotic Drugs 1961<sup>244</sup> concentrated on narcotics control,<sup>245</sup> manufacturing,<sup>246</sup> trade<sup>247</sup> and possession<sup>248</sup> and the Convention on Psychotropic Substances 1971<sup>249</sup> also concentrated on preventing illicit trafficking in drugs through international co-operation.<sup>250</sup> Instead, the Vienna Convention focused on the confiscation and forfeiture of drugs-related money laundering, stating under Article 5 that; “[e]ach party shall adopt such measures as may be necessary to enable confiscation of: (a) Proceeds derived from offences in accordance with article 3, paragraph 1...”<sup>251</sup> and providing legal tools to confiscate assets derived from drugs trafficking, through freezing and forfeiture, under Article 5(2) and 5(4).<sup>252</sup> Furthermore,

---

<sup>242</sup> UN Treaty Series vol. 1582 No. 27627 Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (‘Vienna Convention’), Article 3(i)(b) although it specifically states that criminalisation is in specific connection with drugs trafficking under Article 3(a); *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 180; Gurulé, J. *The 1988 U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances – A Ten Year Perspective: Is International Cooperation Merely Illusory?* (1998-1999) 22 Fordham International Law Journal 75, 80; Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1131; Stewart, D.P. *Internationalizing the War in Drugs: The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (1989-1990) 18 Denver Journal of International Law and Policy 388, 392.

<sup>243</sup> *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 182.

<sup>244</sup> As amended by the 1972 Protocol amending the Single Convention on Narcotic Drugs 1961, <[http://www.unodc.org/pdf/convention\\_1961\\_en.pdf](http://www.unodc.org/pdf/convention_1961_en.pdf)> accessed November 2016.

<sup>245</sup> *ibid* Article 2.

<sup>246</sup> *ibid* Article 29.

<sup>247</sup> *ibid* Article 30.

<sup>248</sup> *ibid* Article 33.

<sup>249</sup> *ibid* 1971 Convention, <[http://www.unodc.org/pdf/convention\\_1971\\_en.pdf](http://www.unodc.org/pdf/convention_1971_en.pdf)> accessed November 2016.

<sup>250</sup> *ibid* Article 21(b)-(e).

<sup>251</sup> Vienna Convention Article 5(1).

<sup>252</sup> *ibid* Daley, M.J., 183-184; Stewart, D.P. *Internationalizing the War in Drugs: The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (1989-1990) 18 Denver Journal of International Law and Policy 388, 395.

the Vienna Convention specifically disallows bank secrecy under Article 5(3),<sup>253</sup> enabling courts and competent domestic authorities to access financial records and track transactions which may be evidence of money laundering. As a result, the UN provided legal guidance which countries could use against money laundering.

However, it is evident from the wording of the Vienna Convention that forfeiture and freezing provisions were only to be used against drugs-related money laundering. For example, under Article 3(1), it specifically lists drugs-related offences under paragraph (a) and states under paragraph (b)(i) that it is a criminal offence to transfer property “*knowing that such property is derived from any offence or offences established in accordance with subparagraph a) of this paragraph...*”.<sup>254</sup> Furthermore, as Bachus states, “*slowing down the drugs trade served as the impetus for the first international anti-money laundering measures...*”.<sup>255</sup> Therefore, it is apparent that international AML efforts were focused primarily on the drugs trade, rather than looking at the whole issue of money laundering and other types of crime it may be used to disguise, such as terrorism. As will be noted under section 3.2.3. the UK had already experienced decades of terrorism with the IRA and had specific AML and CTF provisions to target its financing.

---

<sup>253</sup> *ibid* Gurulé, 83; *ibid* Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1133.

<sup>254</sup> *ibid* Vienna Convention Article 3(1)(a) and (b)(i).

<sup>255</sup> Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835, 835; Stessens, G. *Money Laundering: A New International Law Enforcement Model* (Cambridge University Press, 2000), 117.

It was not until 2000 that the UN decided to revisit the issue of finances generated by organised criminal groups,<sup>256</sup> including terrorist financing,<sup>257</sup> by virtue of the Convention against Transnational Organised Crime (“Palermo Convention”).<sup>258</sup> As will be explained in chapter four and under section 3.2.2, this is because the US had begun to experience terrorist acts, and had started to lead international efforts to clamp down on terrorist financing.<sup>259</sup> The Palermo Convention widened the application of financial and legal tools to include predicate offences outside drug trafficking and expressed deep concern regarding “*the growing links between transnational organized crime and terrorist crimes...*”,<sup>260</sup> for example, through al-Qaeda, which had been prevalent throughout the 1990s.<sup>261</sup> Under Article 2(b), the scope of AML regulations for domestic jurisdictions to use was widened from drugs trafficking to “*serious crime*”<sup>262</sup> to which asset forfeiture and freezing were applied under Article 6. Consequently, it was now recognised by the UN that terrorist financing used a mixture of legal and illegal sources of proceeds to fund their ultimate crime. However, it should be noted that the Palermo Convention did not enter into force until *after*

---

<sup>256</sup> As defined through the Palermo Convention, ‘organised criminal groups’ mean “*a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*” from Article 2(a) A/RES/55/25 UN Convention against Transnational Organised Crime (15 November 2000) (‘Palermo Convention’).

<sup>257</sup> Under the UN definition of “terrorism”, spread over nine Conventions and Protocols.

<sup>258</sup> A/RES/55/25 UN Convention against Transnational Organised Crime (15 November 2000) (‘Palermo Convention’)

<<http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>> accessed November 2016.

<sup>259</sup> E.g. The Financial War on Terror; Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Routledge, 2015).

<sup>260</sup> *ibid* A/RES/55/25 UN Convention against Transnational Organised Crime (15 November 2000) (‘Palermo Convention’), [4], 2; [6], 3.

<sup>261</sup> E.g. co-ordinated attacks by al-Qaeda on US Embassies in Kenya and Tanzania in 1998, Federal Bureau of Investigation ‘*East African Embassy Bombings*’ <<https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings>> accessed November 2016.

<sup>262</sup> *ibid*.

9/11,<sup>263</sup> therefore many countries only had to adhere to the minimum requirements of the Vienna Convention in their AML regimes, potentially causing difficulty with international communications and information-sharing on predicate offences outside drugs-trafficking.<sup>264</sup>

As a supranational body with 28 Member States, including the UK, which was founded on the principles of free movement of people and commerce within its boundaries,<sup>265</sup> and that it initiated extensive AML measures before the UN, it is necessary to discuss the European Union (EU) in the context of international action against money laundering. Unlike the UN, the EU started to widen the scope of money laundering to cover all predicate offences, including terrorism, before 9/11. For instance, in 1991, the European Council implemented Directive 91/308 on Prevention of the Use of the Financial System for the purpose of Money Laundering,<sup>266</sup> stating under Article 2 that

---

<sup>263</sup> Entered into force September 29<sup>th</sup> 2003.

<sup>264</sup> However, the International Convention for the Suppression of the Financing of Terrorism 1999 would have also covered money laundering for the purposes of terrorist financing – see paragraph 5 of preamble to the Convention but this was under-used; also the Model Treaty on Mutual Assistance in Criminal Matters was adopted by the General Assembly in December 1998 through Resolution A/RES/53/112 Model Treaty on Mutual Assistance in Criminal Matters was adopted by the General Assembly (December 1998) which encouraged Member States to use mutual legal assistance through information and evidence sharing <[http://www.unodc.org/pdf/model\\_treaty\\_mutual\\_assistance\\_criminal\\_matters.pdf](http://www.unodc.org/pdf/model_treaty_mutual_assistance_criminal_matters.pdf)> accessed November 2016; plus there were some multilateral agreements on Mutual Assistance which included the proceeds of crime in regions, e.g. for Economic Community of West African States a Convention on Mutual Assistance in Criminal Matters was passed in 1992, which included requests for mutual assistance on the forfeitures and confiscations of the proceeds of crime (Article 2(e)); United Nations Treaty Collection *Economic Community of West African States Convention on Mutual Assistance in Criminal Matters* (1992) <<http://treaties.un.org/doc/Publication/UNTS/Volume%202329/Part/volume-2329-I-41737.pdf>> accessed November 2016.

<sup>265</sup> Treaty establishing the European Economic Community (Treaty of Rome) 25 March 1957, Title III, Articles 48-58 (freedom of movement of people); Treaty of Rome, Articles 2, 9-37 (freedom of commerce/movements of goods); <[http://ec.europa.eu/economy\\_finance/emu\\_history/documents/treaties/rometreaty2.pdf](http://ec.europa.eu/economy_finance/emu_history/documents/treaties/rometreaty2.pdf)> accessed November 2016.

<sup>266</sup> Cribb, N. *Tracing and confiscating the proceeds of crime* (2003) 11(2) *Journal of Financial Crime* 168, 174; Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering ('First Money Laundering Directive'). NB. The First Money Laundering Directive has been superseded by Directive 2001/97/EC (4 December 2001) amending Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering ("Second Money Laundering Directive"); Directive 2005/60/EC (26 October 2005) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing ("Third Money Laundering Directive") and Directive

“Member States shall ensure that money laundering as defined in this Directive is prohibited”.<sup>267</sup> This was partly as a reaction to the growing globalisation of the financial system and the effects of banks involved in money laundering, such as BCCI, could have on the regional and global economies.<sup>268</sup> The Directive shifted the investigative burden onto financial institutions<sup>269</sup> so that they took preventative steps on money laundering, including customer identification<sup>270</sup> especially on transactions above ECU 15,000.<sup>271</sup> Furthermore, in 1998, a Joint Action on Money Laundering was launched,<sup>272</sup> requiring Member States to enable other Member States to identify and trace criminal proceeds in their jurisdiction<sup>273</sup> and requiring that best practice was followed by each Member’s judiciary and investigative authorities when co-operating internationally in such investigations.<sup>274</sup> To enable such decisions to be followed, EUROPOL was formed by the EU in 1995,<sup>275</sup> offering advice and support to national law

---

2015/849/EU (20 May 2015) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (‘Fourth Money Laundering Directive’).

<sup>267</sup> *ibid* Directive 91/308/EEC.

<sup>268</sup> Bank of England *Sandstorm Report* (1991) (Wikileaks, redacted version)

<[https://wikileaks.org/wiki/BCCI\\_Sandstorm\\_report,\\_1991](https://wikileaks.org/wiki/BCCI_Sandstorm_report,_1991)> accessed November 2016; Kerry, J. (Sen.) & Brown, H. (Sen.) *The BCCI Affair: A Report to the Committee on Foreign Relations United States Senate* 102d Congress 2d Session Senate Print 102-140 (GPO, December 1992).

<sup>269</sup> *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 188.

<sup>270</sup> Directive 91/308, Article 3(1); *ibid* Cribb, N. *Tracing and confiscating the proceeds of crime* (2003) 11(2) Journal of Financial Crime 168, 174.

<sup>271</sup> *ibid* Article 3(2), Article 4.

<sup>272</sup> *Joint Action of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime* (98/699/JHA)

<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:333:0001:0003:EN:PDF>> accessed November 2016.

NB. Reviewed in Council of the European Union *Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime* (2001/500/JHA) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001F0500:EN:HTML>> accessed November 2016.

<sup>273</sup> *ibid* Directive 91/308 Article 1(3).

<sup>274</sup> *ibid* Article 6.

<sup>275</sup> *European Union Convention drawn up on the basis of Article K.3 of the Treaty on the European Union, on the Establishment of a European Police Office (Europol Convention)* (Official Journal 316, 27 November 1995) <[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41995A1127\(01\):EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41995A1127(01):EN:HTML)> accessed November 2016; Title VI, K.3 (Home



enforcement authorities,<sup>276</sup> as well as promoting information-sharing to combat organised crime<sup>277</sup> based on mutual legal assistance (MLA). Consequently, the EU highlighted the benefits of MLA and international co-operation, as well as a comprehensive AML regime, which was not limited to the trafficking of drugs.

Despite its narrow field of application, the Vienna Convention also resulted in a number of international organisations being set up as part of AML efforts, which led the way in providing international “best practice” on AML. Primarily, the Financial Action Task Force (FATF) was set up by the “Group of 7” (G-7)<sup>278</sup> in 1989, subsequently applying 40 Recommendations in 1990 to combat money laundering under the Vienna Convention,<sup>279</sup> although these were non-binding.<sup>280</sup> For example, the Recommendations include *inter alia* measures on customer identification and record-keeping in financial institutions<sup>281</sup> and suspicious activity reports on large and unusual

---

Affairs and Justice) of the Treaty on the European Union (Maastricht Treaty) 7 February 1992, Official Journal C 191 (29 July 1992);  
<<http://eur-lex.europa.eu/en/treaties/dat/11992M/htm/11992M.html#0001000001>> accessed November 2016.

<sup>276</sup> *ibid* Europol Convention Article 2(1) on objectives; Article 3(2).

NB. Replaced by Council of the European Union *Council Decision on Establishing the European Police Office (Europol)* (2009/371/JHA) (6 April 2009)

<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:EN:PDF>> accessed November 2016; EUROPOL Website:

<<https://www.europol.europa.eu/activities-services/services-support>>, accessed April 2018.

<sup>277</sup> *ibid* Europol Convention Article 3(1).

<sup>278</sup> In 1989, it was the Group of 7, it increased to the Group of 8 with Russia, and is now the Group of 7 with the expulsion of Russia *ibid*; Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1138; United Kingdom and United States are members of the Financial Action Task Force:

<[http://www.fatf-gafi.org/document/52/0,3343,en\\_32250379\\_32236869\\_34027188\\_1\\_1\\_1\\_1,00.html](http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32236869_34027188_1_1_1_1,00.html)> accessed November 2016; Saudi Arabia is a member of the Middle East North Africa Financial Action Task Force (MENAFATF) which recognises FATF Recommendations as the accepted standard for Anti-Money Laundering/Counter-Terrorist Financing enforcement  
<<http://www.menafatf.org/categoryList.asp?cType=about>> accessed November 2016.

<sup>279</sup> Financial Action Task Force *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012, updated February 2018) Recommendation 1 [1]

<<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>> accessed April 2018.

<sup>280</sup> See chapter three, 3.2.1. *supra*.

<sup>281</sup> *ibid* FATF Recommendations 5 and 10.

transactions,<sup>282</sup> preventing bank secrecy and enabling authorities to track suspicious financial transactions relating to money laundering. In addition, the FATF Recommendations ensure that confiscation and freezing procedures mentioned in the Convention were carried out<sup>283</sup> by establishing its cornerstone of compliance – peer and political pressure between member countries<sup>284</sup> - through Mutual Evaluation Reports.<sup>285</sup> Furthermore, in 1996, the FATF extended its remit on money laundering to include criminal offences outside the Convention’s narrow mandate on drugs-related money laundering.<sup>286</sup>

Secondly, the Egmont Group on Financial Intelligence Units (FIU) were established,<sup>287</sup> ensuring mutual assistance between countries’ FIU<sup>288</sup> on AML provisions and information sharing. Moreover, other organisations such as the Bank for International Settlements through Basel Committee on Banking Regulations and Supervisory Practices brought out measures to prevent “dirty money” flowing through

---

<sup>282</sup> *ibid* FATF Recommendation 20.

<sup>283</sup> *ibid* FATF Recommendation 4; *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 186.

<sup>284</sup> E.g. Recommendations 18 & 19; Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835, 852.

<sup>285</sup> *ibid* Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1139 – mutual country assessments established after FATF Second Report in 1991; *ibid* Bachus, 851; also endorsed by International Monetary Fund and World Bank post-9/11, Schott, P. *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2<sup>nd</sup> Edition, The International Bank for Reconstruction and Development, World Bank & International Monetary Fund, 2009), X-2-X-3, <[http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference\\_Guide\\_AMLCFT\\_2ndSupplement.pdf](http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf)> accessed April 2018.

<sup>286</sup> *ibid* FATF Recommendations Introduction, 2, para. 4; Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 Tul. Journal Int’l & Comp. Law 161, 174.

<sup>287</sup> All countries referred to in this thesis, are members of the Egmont Group on Financial Intelligence Units –Saudi Arabia: Wehdat Altahariyat Al Maliyah Saudi Arabia Financial Investigations Unit, United Kingdom: National Crime Agency, United States: Financial Crimes Enforcement Network (FinCEN) Egmont Group *List of Members* <<https://www.egmontgroup.org/en/membership/list>> accessed April 2018.

<sup>288</sup> Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835, 855.

financial institutions. In the Basel Committee's Statement of Principles 1988,<sup>289</sup> the main task for financial institutions was to “*adopt a common position in order to ensure that banks are not used to hide or launder funds acquired through criminal activities...*”<sup>290</sup> and prevent bank secrecy by introducing guidelines to banks, such as customer identification<sup>291</sup> and compliance with law enforcement authorities.<sup>292</sup> Additionally, the International Monetary Fund (IMF), of which all sample countries are members,<sup>293</sup> used their powers of surveillance on members' economies<sup>294</sup> to evaluate whether they were conforming to international money laundering standards since early 2001,<sup>295</sup> as well as providing technical assistance, information sharing and developing and promoting common policies between countries.<sup>296</sup> Furthermore, a meeting of the world's leading multinational banks in 2000<sup>297</sup> resulted in the formation of the Wolfs-berg Principles, which sought “*create a common standard to reduce the uncertainties and complexities resulting from running multinational banks across disparate anti-*

---

<sup>289</sup> Basel Committee on Banking Regulations and Supervisory Practices Statement of Principles, (12 December 1988), Bank for International Settlements *PREVENTION OF CRIMINAL USE OF THE BANKING SYSTEM FOR THE PURPOSE OF MONEY-LAUNDERING* (December 1988) <<https://www.bis.org/publ/bcbssc137.pdf>> accessed April 2018.

<sup>290</sup> *ibid* Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1136.

<sup>291</sup> Basel Committee Principle II; *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 185.

<sup>292</sup> Basel Committee Principle IV.

<sup>293</sup> International Monetary Fund *Members* <<http://www.imf.org/external/np/sec/memdir/members.htm>> accessed November 2016.

NB. IMF has “near universal membership” of 187 countries, <<http://www.imf.org/external/np/exr/facts/surv.htm>> accessed November 2016.

<sup>294</sup> Through annual evaluations with a member's Government and Central Bank – s. 3 Article IV International Monetary Fund Articles of Agreement 1944 (amended effective 1969, 1978, 1992, 2009) <<http://www.imf.org/external/pubs/ft/aa/aa04.htm>> accessed November 2016.

<sup>295</sup> International Monetary Fund *IMF Role in Anti Money Laundering/Counter-Terrorist Financing* <<http://www.imf.org/external/np/exr/facts/aml.htm>> accessed November 2016.

<sup>296</sup> *ibid*.

<sup>297</sup> Haynes, A. *The Wolfsberg Principles: An Analysis* (2004) 7(3) Journal of Money Laundering Control 207, 207.

*laundrying regimes*”.<sup>298</sup> For instance, the identification of customers was required,<sup>299</sup> as well as a formulation of practices when identifying suspicious activities<sup>300</sup> and monitoring of transactions by banks.<sup>301</sup> As a result, it was evident that many international organisations and financial institutions were working together to prevent the flow of the proceeds of crime.<sup>302</sup>

However, it should be noted that the organisations mentioned above do not have legally binding measures, instead creating “soft law”.<sup>303</sup> This suggests that many countries did not have to implement specific AML legislation,<sup>304</sup> although the FATF Recommendations have proved to be more popular than the Vienna Convention, with more than 180 jurisdictions endorsing them.<sup>305</sup> Consequently, the international AML regime before 9/11 was not necessarily followed by all sovereign states, creating a *mélange* of legislation and Mutual Legal Assistance (MLA) treaties which may not have been recognised internationally.<sup>306</sup>

---

<sup>298</sup> *ibid.*

<sup>299</sup> Wolfsberg Principle 1.2, <<https://www.wolfsberg-principles.com/publications/wolfsberg-standards>> accessed April 2018; *ibid* Haynes, A. *The Wolfsberg Principles: An Analysis* (2004) 7(3) *Journal of Money Laundering Control* 207, 208-210.

<sup>300</sup> *ibid* Wolfsberg Principle 4.

<sup>301</sup> *ibid* Principle 5.

<sup>302</sup> No inclusion of the World Bank as it started work on country assessments in November 2002, Schott, P. *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2<sup>nd</sup> Edn. The International Bank for Reconstruction and Development, World Bank & International Monetary Fund, 2009), X-2-3.

<sup>303</sup> At its very basic level, ‘soft law’ is defined as “*normative provisions contained in non-binding texts*” Shelton, D, ed. *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System*. (Oxford University Press, 2000), 292; Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 *Arizona Journal of International and Comparative Law* 835, 851; *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 *St. Louis-Warsaw Transatlantic Law Journal* 175, 184.

<sup>304</sup> Chapter three, 3.5.

<sup>305</sup> As opposed to 190 which are party to the Vienna Convention, *UN Treaties Collection* <[http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=VI-19&chapter=6&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=VI-19&chapter=6&lang=en)> accessed November 2016; Financial Action Task Force *Annual Report (2009-2010)*, 9 <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatfannualreport2009-2010.html>> accessed April 2018.

<sup>306</sup> NB. There has been some success with the international AML regime – see in general Ryder, N. *Financial Crime in the 21<sup>st</sup> Century: Law and Policy* (Edward Elgar, 2011), 13-19.

### 3.2.1.1. The move towards counter-terrorist financing

Although the UN's AML Convention was narrowly defined, it promoted international co-operation against terrorist financing before 9/11. For example, in 1996, the UN General Assembly introduced Resolution A/RES/51/210 which stated at s3(f) that Member States were to "*take steps to prevent and counteract, through appropriate domestic measures, the financing of terrorists and terrorist organizations...*".<sup>307</sup> However, the two draft Conventions arising out of this resolution only covered terrorist bombings and nuclear terrorism.<sup>308</sup> As Levi explains, "[t]he Committee's initial mandate did not include the financing of terrorism",<sup>309</sup> nevertheless, it was encouraged by the US to include CTF within its remit, especially after the 1998 Kenya and Tanzania Embassy bombings.<sup>310</sup> Consequently, the UN passed Resolutions A/RES/52/165 in 1997 and A/RES/53/108 in 1999 which highlighted the need to counter terrorist financing as well as a suggestion to form a Convention against the financing of terrorism.<sup>311</sup>

---

<sup>307</sup> A/RES/51/210 Measures to eliminate international terrorism (17 December 1996) <<http://www.un.org/documents/ga/res/51/a51r210.htm>> accessed November 2016; A/RES/45/121 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (14 December 1990).

NB. General Assembly Resolutions are generally seen as non-binding to Member States and international law, and it is up to the Member States to apply them – rather, they are 'recommendations' to Member States; Schwebel, S.M. *The Effect of Resolutions of the General Assembly on Customary International Law* (1979) 73 American Society of International Law Proceedings 301, 301.

<sup>308</sup> Levi, M. *Combating the Financing of Terrorism: A History and Assessment of the Control of Threat Finance* (2010) 50(4) British Journal of Criminology 650, 652.

<sup>309</sup> *ibid* Levi.

<sup>310</sup> *ibid* Levi.

<sup>311</sup> A/RES/52/165 Measures to eliminate international terrorism (15 December 1997), para. 3 on pledge to prevent terrorist financing <[http://www.un.org/ga/search/view\\_doc.asp?symbol=A/Res/52/165](http://www.un.org/ga/search/view_doc.asp?symbol=A/Res/52/165)> accessed November 2016; A/RES/53/108 Measures to eliminate international terrorism (26 January 1999), para. 11, on a draft International Convention against terrorist financing, <[http://www.un.org/ga/search/view\\_doc.asp?symbol=a/res/53/108](http://www.un.org/ga/search/view_doc.asp?symbol=a/res/53/108)> accessed November 2016.

In 1999, therefore, the UN introduced an important international instrument in the struggle against terrorist financing – the International Convention for the Suppression of the Financing of Terrorism.<sup>312</sup> This was a major move towards international co-operation against terrorism and its financing, by criminalising the collection or distribution of funds which were to be used in an act of terrorism,<sup>313</sup> and also outlined measures for freezing and forfeiture of funds used for terrorist acts.<sup>314</sup> Furthermore, the Convention sets out minimum standards on customer identification requirements for banks, also known as ‘know your customer’ (KYC), such as regulations for the prohibition of the opening of accounts whereby the holder or beneficiary is unidentified or unidentifiable,<sup>315</sup> reporting of suspicious transactions<sup>316</sup> and the maintenance of customer transactions for at least five years.<sup>317</sup> However, the Convention abjectly fails to define “terrorism”,<sup>318</sup> instead relying on no fewer than nine Conventions and Protocols to outline what it means,<sup>319</sup> potentially causing different interpretations to

---

<sup>312</sup> International Convention for the Suppression of the Financing of Terrorism, adopted by the General Assembly of the United Nations in Resolution A/RES/54/109 (9 December 1999).

<sup>313</sup> Article 2(1)(a) and (b), also request under Article 4 for domestic states to criminalise terrorist financing, 1999 United Nations Convention for the Suppression of Terrorist Financing, <<http://www.un.org/law/cod/finterr.htm>> accessed November 2016, adopted by UN in Resolution A/RES/54/109 (9 December 1999).

<sup>314</sup> *ibid* Article 8.

<sup>315</sup> *ibid* Article 18(i).

<sup>316</sup> *ibid* Article 18(iii).

<sup>317</sup> *ibid* Article 18(iv).

<sup>318</sup> Phillips, A. *Terrorist Financing Laws won't wash: It ain't money laundering* (2004) 23 University of Queensland Law Journal 81, 85-87.

<sup>319</sup> *ibid* Phillips, A., 85; Annex to the 1999 Convention: UN Treaty Series 1973 *Convention for the Suppression of Unlawful Seizure of Aircraft* (16 December 1970); 974 UN Treaty Series 177 *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (23 September 1971); A/RES/3166 (XVIII) *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (14 December 1973); A/RES/34/146 *International Convention against the Taking of Hostages* (17 December 1979); INFCIRC/274 *Convention on the Physical Protection of Nuclear Material* (3 March 1980); 474 UN Treaty Series 1990 No. 14118 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (24 February 1988); 1678 UN Treaty Series 1992 No.29004 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (10 March 1988); 1678 UN Treaty Series 1992 No.29004 *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf* (10 March 1988); A/RES/52/164 *International Convention for the Suppression of Terrorist Bombings* (15 December 1997).

be drawn by domestic states.<sup>320</sup> The UN itself has stated that this is because it “*has been constrained by the inability of Member States to agree on an anti-terrorism convention including a definition of terrorism.*”<sup>321</sup> Moreover, as Leong notes, although the Convention was introduced 18 months before the events of 9/11, only 41 Member States had signed the Treaty and, out of that, 6 had ratified it.<sup>322</sup> This ambivalence towards combating terrorism is illustrated in UN Security Council Resolution 1269,<sup>323</sup> which emphasised the need for states to take appropriate action against terrorism but was not adhered to internationally as it was not mandatory.<sup>324</sup> As Ward notes, “[m]ost countries lacked capacity to take appropriate measures to combat terrorism and co-operate with each other, and many lacked political will to take any

---

<sup>320</sup> E.g. United Kingdom definition of terrorism falls under s. 1 (s. 1-4) Terrorism Act 2000 c.11 – criticised by UK House of Commons and House of Lords Joint Committee on Human Rights as being broad enough to capture “speech or actions” concerning resistance to an oppressive regime overseas; Parliamentary Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters* 3rd Report of Session 2005-2006 (HMSO, 28 November 2005), 13, para. 12 <<http://www.publications.parliament.uk/pa/jt200506/jtselect/jtrights/75/75i.pdf>> accessed November 2016.; inclusion of “encouragement” as an act of terrorism in s. 1 of the Terrorism Act 2006 c.11 has been criticised by organisations such as Liberty; Liberty *Liberty’s response to Lord Carlile’s review of the definition of terrorism* (June 2006), 7 <<http://www.liberty-human-rights.org.uk/pdfs/policy06/response-to-carlile-review-of-terrorism-definition.pdf>> accessed November 2016.

<sup>321</sup> United Nations *Terrorism* <<https://www.un.org/News/dh/infocus/terrorism/sg%20high-level%20panel%20report-terrorism.htm>> accessed November 2016.

<sup>322</sup> Mei Leong, A., *Chasing Dirty Money: domestic and international measures against money laundering*, (2007) 10(2) *Journal of Money Laundering Control* 140-156, 145.  
NB. However, this author contends that 42 countries signed the Convention and only 4 had ratified it before 9/11; United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999) <[http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=XVIII-11&chapter=18&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en)> accessed November 2016.

<sup>323</sup> S/RES/1269 (1999) Responsibility of the Security Council in the maintenance of international peace and security <<https://www.un.org/Docs/scres/1999/sc99.htm>> accessed November 2016.

<sup>324</sup> Ward, C.A. *Building Capacity to Combat Terrorism: The Role of the United Nations Security Council* (2003) 8(2) *Journal of Conflict & Security Law* 289, 290.

*action whatsoever.*"<sup>325</sup> Consequently, until the introduction of Security Council Resolution 1373,<sup>326</sup> which made it a mandatory requirement to adopt regulatory frameworks to combat terrorist financing,<sup>327</sup> it was not a priority for many countries. As a result, although the Convention and UN efforts in the 1990s became central to international endeavours against terrorist financing, most Member States had simply failed to either sign the Convention or ratify its provisions before 9/11.

### **3.2.2. The United States**

As the self-proclaimed leading jurisdiction behind international efforts on both money laundering and terrorist financing post-9/11,<sup>328</sup> it is necessary to discuss the US first. Prior to 9/11, the US efforts against financial crime were mainly concentrated on money laundering.<sup>329</sup> Before any UN recommendations on this area were formulated, the US had already developed a framework of AML statutes which covered all predicate offences. During the 1960s and 1970s, the US launched its first generation of statutes which aimed to prevent any profits gained by criminal enterprise from being used in the formal financial system. For example, the Racketeer Influenced and Corrupt Organizations Act of 1970 (RICO) first outlawed the proceeds of racketeering

---

<sup>325</sup> *ibid* Ward, C.A., 290.

<sup>326</sup> NB. Unlike General Assembly Resolutions, which are recommendations, under Article 25 of the UN Charter Members "*agree to accept and carry out the decisions of the Security Council in accordance with the present Charter*", meaning that they are legally binding on Member States; UN Charter <[www.un.org](http://www.un.org)> accessed November 2016.

<sup>327</sup> *ibid* 294-295.

<sup>328</sup> The Whitehouse Archives *President Freezes Terrorists' Assets* (24 September 2001) <<https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>> accessed November 2016; Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Routledge, 2015), 2.

<sup>329</sup> NB. The US also concentrated on fraud and insider trading: 18 U.S.C. Chapter 47 – Fraud and False Statements (fraud); Securities Act of 1933 (Title I of Pub. L. 73-22, 48 Stat. 74), 15 U.S.C. §77; Securities Exchange Act of 1934 (Pub.L. 73-291, 48 Stat. 881), 15 U.S.C. §78 (Rule 10b-5) (insider trading); *Chiarella v. United States* (1980) 445 U.S. 222.



from being invested into the US economy,<sup>330</sup> as a weapon in the US armoury against the rise of the Mafia families, which had gained strangleholds in labour unions and the gambling mecca of Las Vegas.<sup>331</sup> Furthermore, RICO established the financial sanction of mandatory forfeiture of any assets if found guilty of racketeering,<sup>332</sup> allowed freezing orders on assets while a criminal trial was being carried out,<sup>333</sup> and enabled seizure of property transferred to a third party.<sup>334</sup> Consequently, the US made its first steps towards attacking “*the economic roots of racketeering activities...*”.<sup>335</sup>

Coupled with RICO, the Bank Secrecy Act of 1970 was introduced, originally known as the Financial Reporting and Currency and Foreign Transaction Reporting Act,<sup>336</sup> to prevent financial institutions from being used to protect the flow of illegal money, again a direct reaction to the Mafia’s influence on both the licit and illicit economies.<sup>337</sup> Spread over a number of Titles in the United States Code,<sup>338</sup> the Bank Secrecy Act initiated customer identification measures,<sup>339</sup> reports on suspicious currency transactions,<sup>340</sup> reporting on domestic transactions over \$10,000<sup>341</sup> as well as reports on importing and exporting of monetary instruments to foreign banks over the

---

<sup>330</sup> §1962(a) Chapter 96, Title 18, United States Code; RICO: Paik, J.S. *RICO* (1988) 26 American Criminal Law Review 971; Franklin, A. Schorr L. & Shapiro D. *Racketeering Influenced Corrupt Organizations* (2008) 45 American Criminal Law Review 921.

<sup>331</sup> Jacobs, J.B. *Mobsters, Unions, and Feds: The Mafia and the American Labor Movement* (1st Edn. New York University Press, 2006); Raab, S. *Five Families: The Rise, Decline, and Resurgence of America's Most Powerful Mafia Empires* (1<sup>st</sup> Edn. Chyrisalis Books Group, 2006).

<sup>332</sup> §1963(a), (b) and (c), Chapter 96, Title 18 U.S.C.; *ibid* Franklin, Schorr & Shapiro, 903.

<sup>333</sup> §1963(d) Chapter 96 Title 18 U.S.C.; *ibid* Franklin, Schorr & Shapiro, 904-905.

<sup>334</sup> §1963(c) Chapter 96 Title 18 U.S.C.

<sup>335</sup> *ibid* Franklin, Schorr & Shapiro, 903.

<sup>336</sup> 31 U.S.C. §5311.

<sup>337</sup> G. Robert Blakey traces this back to the Kefauver and McClellan investigations of the Mafia in the 1950s and 1960s, and credits Sen. McClellan with the precursor to the RICO Act, McClellan, J.L. (Sen.) *A bill to Outlaw the Mafia or Other Organized Crime syndicates* S. 2187, 89th Congress, (GPO, 24 June 1965) . Blakey, G.R. *Rico: The Genesis of an Idea Trends in Organized Crime* (2006) Vol. 9, No. 8, 9-10.

NB. G. Robert Blakey is the architect of RICO.

<sup>338</sup> Titles 12, 15, 18 and 31 of United States Code.

<sup>339</sup> §5325 Title 31 U.S.C.

<sup>340</sup> §5311 Title 31 U.S.C.

<sup>341</sup> §5313 Title 31 U.S.C.

same amount.<sup>342</sup> As a result, the US had a clear framework in place to counteract the flow of illegal finances prior to international action in the 1980s.

Nevertheless, although there were some successes in preventing both individuals and financial institutions from hiding illicit funds within the financial system,<sup>343</sup> and a drive by the Treasury Department, Internal Revenue Service and the Department of Justice to utilise its provisions during the 1980s in Operation Greenback,<sup>344</sup> the Bank Secrecy Act attracted some criticism. Primarily, the Bank Secrecy Act was initially intended to tackle income tax evasion,<sup>345</sup> not just money laundering, therefore some aspects particular to the crime of money laundering were not caught by the Act. For example, reporting requirements could be bypassed by money launderers through ‘structuring’, or the deposit of many cash transactions below the \$10,000 limit, a point unintentionally endorsed by the US courts through their narrow interpretation of the requirement.<sup>346</sup> For instance, in *United States v Anzalone*,<sup>347</sup> the court decided that the Act “*did not specifically prohibit dividing a large transaction into several smaller transactions to circumvent the reporting requirement...*”.<sup>348</sup> This position was confirmed in *United States v Varbel*<sup>349</sup> and *United States v Denmark*,<sup>350</sup> highlighting the difficulties in applying the Act in cases where transactions were structured. Moreover, the Act only applied to specified financial institutions,<sup>351</sup> “*leaving money launderers*

---

<sup>342</sup> §5316 Title 31 U.S.C.

<sup>343</sup> *United States v. Thompson* 603 F.2d 1200 (5<sup>th</sup> Cir 1979); *United States v. First National Bank of Boston* CR 85 52-MA (D. Mass February 7 1985).

NB First National Bank of Boston pleaded guilty to Bank Secrecy offences.

<sup>344</sup> Villa, J.K. *A Critical View of Bank Secrecy Act Enforcement and the Money Laundering Statutes* (1987-1988) 37 Catholic University Law Review 489, 492.

<sup>345</sup> Blaut, M.S. *Banking Secrecy – The End of an Era?* (1975) 3 Syracuse Journal of International Law 271, 271; 286-290.

<sup>346</sup> Strafer, G.R. *Money Laundering: The Crime of the 90s* (1989-1990) 27 American Criminal Law Review 149, 159-160.

<sup>347</sup> *United States v. Anzalone* 766 F.2d 676 (1<sup>st</sup> Cir 1985).

<sup>348</sup> *ibid* [20].

<sup>349</sup> *United States v. Varbel* 780 F.2d 758 (9<sup>th</sup> Cir 1986) [26].

<sup>350</sup> *United States v. Denmark* 779 F.2d 1559 (11<sup>th</sup> Cir 1986) [21].

<sup>351</sup> See *California Bankers' Association v. Schultz* 416 U.S. 21 (1974), 416; U.S. 22, 58, 69-70.

*free to employ currency exchange houses and any other non-bank financial service to make transactions of any dollar amount... ”.*<sup>352</sup> As a result, the effectiveness of the Act in cases of money laundering was low,<sup>353</sup> with the Treasury Department also failing to enforce the reporting requirements properly.<sup>354</sup>

Due to gaps within the Bank Secrecy Act, the second generation of AML legislation was launched in the US, through the Money Laundering Control Act of 1986 (MLCA). It was not until the introduction of the MLCA that money laundering derived from a specific unlawful act in the US Code was criminalised.<sup>355</sup> Under the MLCA, it became a federal offence for anyone to knowingly promote concealment of such finances,<sup>356</sup> as well as structuring transactions in order to avoid the Bank Secrecy Act’s reporting requirements,<sup>357</sup> thereby countering previous criticisms of the Bank Secrecy Act. Furthermore, banks and financial institutions were specifically targeted under §1957,<sup>358</sup> imposing criminal and civil liability on financial institutions and their employees if they knew a transaction over \$10,000 was “criminally derived”.<sup>359</sup> Moreover, during the 1990s, the US further strengthened its AML regime through the

---

NB. The overall provisions of the Bank Secrecy Act were upheld in *Schultz*.

<sup>352</sup> *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175,189-190.

<sup>353</sup> *ibid* 190.

<sup>354</sup> *ibid*.

<sup>355</sup> §1956 Money Laundering Control Act of 1986 (Pub. L. 99-570, 100 Stat. 3207) (18 U.S.C. Ch. 95); *ibid* Gurulé, 97; Newland, L.S. *Money Laundering* (2008) 45 American Criminal Law Review 741, 754.

<sup>356</sup> §1956(a)(1)(B)(i) Money Laundering Control Act of 1986; *ibid* Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 Tul. Journal Int’l & Comp. Law 161, 186; Gurulé, 98.

<sup>357</sup> Commonly known as ‘smurfing’ - §1956(a)(1)(B)(ii) Money Laundering Control Act of 1986 and amendment to §1354 of Currency and Transactions Reporting Act to impose civil and criminal liability; Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 Tul. Journal Int’l & Comp. Law 161, 186; Crocker, T.E. & Bellinger, J.B. *New US Anti-Money Laundering Legislation* (1987) 6 International Financial Law Review 33, 35; *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 189.

<sup>358</sup> *ibid* Crocker & Bellinger, 34.

<sup>359</sup> *ibid* Crocker & Bellinger, 34.

Annunzio-Wylie Anti-Money Laundering Act of 1992-<sup>360</sup> most notably introducing Suspicious Activity Reports as part of financial institutions' record keeping liabilities.<sup>361</sup> Additionally, the civil and criminal liabilities of bank secrecy provisions were extended to Money Services Businesses under the Money Laundering Suppression Act of 1994<sup>362</sup> and a National Anti-Money Laundering Strategy was launched under the Money Laundering and Financial Crimes Strategy Act of 1998.<sup>363</sup> Consequently, US legislation increased regulatory burden on banks to investigate and report suspicious transactions. This was criticised on the basis of cost to financial institutions and the private sector as well as breaching customer confidentiality,<sup>364</sup> a problem reflected in jurisdictions such as the United Kingdom and Australia.<sup>365</sup> As a result, it was apparent that, before 9/11 and even before the international response towards controlling

---

<sup>360</sup> Annunzio-Wylie Anti-Money Laundering Act of 1992 (under Title XV of the Housing & Community Development Act 1992) (Pub. L. 102-358, 106 Stat. 3672).

<sup>361</sup> §1517 Annunzio-Wylie Anti-Money Laundering Act of 1992 (under Title XV of the Housing & Community Development Act 1992) (Pub. L. 102-358, 106 Stat. 3672); Financial Crime Enforcement Network (FinCEN) *History of Anti-Money Laundering Laws* <<https://www.fincen.gov/history-anti-money-laundering-laws>> accessed April 2018.

<sup>362</sup> §407 and §408 Money Laundering Suppression Act of 1994 (under Title IV of the Riegle-Neal Community Development and Regulatory Act 1994) (Pub. L. 103-325 Title IV, 108 Stat. 2243) (31 U.S.C. 5301).

<sup>363</sup> §2 Money Laundering and Financial Crimes Strategy Act of 1998 (Pub. L. 105-310, 112 Stat. 2941) (18 U.S.C. Ch. 46).

<sup>364</sup> Alford, D.E. *Anti-Money Laundering Regulations: A Burden on Financial Institutions* (1993-1994) 19 North Carolina Journal of International Law and Commercial Regulation 437, 466-467; 456-466 (US anti-money laundering legislation).

<sup>365</sup> In the UK, the Law Society criticised the SARs regime in relation to the cost of regulatory burdens on the private sector (especially law firms) to the House of Lords European Union Committee 19<sup>th</sup> Report of Session 2008-9 *Money Laundering and the Financing of Terrorism Volume II: Evidence* (HMSO, July 2009), 15, 7.3.4.-7.3.7 <<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldcom/132/132i.pdf>> accessed November 2016, especially with regard to additional costs needed to monitor transactions including staffing and hours of work spent on requirements – ‘*These hidden costs are felt more keenly by those parts of the regulated sector where transactions are not mere numbers and ongoing monitoring is not susceptible to automated processes. What is clear is that the private sector is investing more in the UK's anti-money laundering regime than the UK government is recovering because of it.*’ (para. 7.3.7.), <<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldcom/132/132i.pdf>> accessed November 2016; Fisher, J. Memorandum to the European Union Committee ‘*There is no doubt that certain sections of the regulated sector (typically financial institutions, law firms and the larger firms of accountants) are devoting significant financial resources to the implementation of anti-money laundering and counter-terrorism procedures... What is more, there is a clear perception amongst those operating in the regulated sector that compliance costs are greater in the United Kingdom than elsewhere in the world due to the stringent way in which Part 7 of the Proceeds of Crime Act 2002 has been drafted, when read*

money laundering, the US had an assertive legislative response towards financial crime, although there were concerns about balancing the need for criminal investigation against the commercial needs of financial institutions.

### **3.2.2.1. The move towards counter-terrorist financing**

Although it is evident that the US had made major improvements to legislation pertaining to the control of money laundering, it is also apparent that legislation devoted to the detection and prevention of terrorist financing before 9/11 was not comprehensively applied. Despite a serious warning in 1993 with the first World Trade Centre bombings,<sup>366</sup> the US still remained largely ambivalent towards CTF and prevention of such acts, rather focusing on the prosecution of the perpetrators,<sup>367</sup> as well as foreign policy towards states who sponsored terrorism.<sup>368</sup> It was even subsequently revealed by the main financier and planner of 9/11, Khalid Sheik Mohammed<sup>369</sup>, that he had financed part of the 1993 operation<sup>370</sup> although, apparently, the funding for the attacks

---

together with the Money Laundering Regulations 2007...’ paras. 4-5 Fisher, J. *Memorandum to the European Union Committee* (HMSO, 20 February 2009) <<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldcom/132/132we11.htm>> accessed November 2016.

For Australia, Sathye, M. *Estimating the cost of compliance of AMLCTF for financial institutions in Australia* (2008) 15(4) *Journal of Financial Crime* 347 who estimated the cost of implementing regulation in 2007 to be A\$1.02billion across the financial sector, 361.

<sup>366</sup> *United States v. Yousef* 925 F. Supp. 1063 (S.D.N.Y.) (1996); *United States v. Yousef* 327 F. 3d 56 (2<sup>nd</sup> Cir 2003); Federal Bureau of Investigation *Famous Cases* - <<https://www.fbi.gov/history/famous-cases/world-trade-center-bombing-1993>>, accessed April 2018; *9/11 Commission Report* (22 July 2004) 71-74, <<http://www.9-11commission.gov/>>, accessed November 2016.

<sup>367</sup> *9/11 Commission Report* (22 July 2004), 72-73 <<http://www.9-11commission.gov/>> accessed November 2016 (regarding prosecution and underestimation of the attack).

<sup>368</sup> Economic and political sanctions against Libya and Iran, who were thought to be state sponsors of terrorism, under the Iran Libya Sanctions Act of 1996 (Pub. L. 104-172 110 Stat. 1541) (50 U.S.C. Ch. 35, 1701 et seq.) <[http://www.fas.org/irp/congress/1996\\_cr/h960618b.htm](http://www.fas.org/irp/congress/1996_cr/h960618b.htm)>, accessed November 2016.

<sup>369</sup> NB. he was also the uncle of Ramzi Yousef, one of the 1993 bombers; *9/11 Commission Report* (22 July 2004), 145 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>370</sup> American Civil Liberties Union *Khalid Sheik Mohammed Combatant Status Review Tribunal Guantanamo Bay* (10 March 2007) <[https://www.aclu.org/files/pdfs/safefree/csrt\\_ksm.pdf](https://www.aclu.org/files/pdfs/safefree/csrt_ksm.pdf)> accessed April 2018; also see example of company transporting Mecca holy water financing 1993 attacks in Levitt, M. *The Political Economy of Middle East Terrorism* (2002) *Middle East Review of International Affairs* Vol. 6 No. 4 <<http://www.washingtoninstitute.org/policy-analysis/view/the-political-economy-of-middle-east-terrorism>> accessed April 2018.

was insufficient.<sup>371</sup> However, there were some steps towards countering specific types of terrorist financing in the US prior to 9/11. In 1917, during World War I, the Trading with the Enemy Act was introduced,<sup>372</sup> allowing the President to regulate, investigate or prohibit foreign financial transactions through the use of an Executive Order,<sup>373</sup> however, this was limited to times of war.<sup>374</sup> After the World Trade Center bombings in 1993, the Violent Crime Control and Law Enforcement Act of 1994 was announced, first introducing material support to terrorism provisions in Title 18 of the US Code.<sup>375</sup> Furthermore, through former US President Bill Clinton's Executive Orders in the mid-1990s,<sup>376</sup> the CTF strategy of the US gathered pace. For example, in 1995, Clinton

---

NB. the admission of former US President George Bush of "waterboarding" Mohammed in his time at Guantanamo Bay was outlined in the aftermath of this interview therefore there are concerns about the accuracy of Mohammed's confessions; Owen, P. (The Guardian 3 June 2010) *George Bush admits US waterboarded 9/11 mastermind* <<http://www.guardian.co.uk/world/2010/jun/03/george-bush-us-waterboarded-terror-mastermind>> accessed November 2016.

<sup>371</sup> Parachini, J. *The World Trade Center Bombers* (1993) (Jonathan B. Tucker (ed.) *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge MA: MIT Press, 2000), 185-206, 194-195 – Ramzi Yousef alleged to have stated to Secret Service Agent Brian Parr that he would have placed sodium cyanide in the bomb canisters had they had enough money (Direct Examination of Brian Parr, *United States of America v Ramzi Ahmed Yousef and Eyud Ismoil*, S1293CR.180 (KTD), October 22, 1997, 4734-4735) – plus the author surmises that the timing of the bombing was due to a lack of funds by the end of the month. The bombers also originally intended to kill 250,000 people by toppling one tower into the other; *Statement By J. Gilmore Childers, Esq. Orrick, Herrington & Sutcliffe LLP New York City, New York and Henry J. DePippo, Esq. Nixon Hargrave Devans & Doyle Rochester, New York, 6(b). Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information Hearing on "Foreign Terrorists in America: Five Years After the World Trade Center"* (February 24, 1998) <[http://www.fas.org/irp/congress/1998\\_hr/s980224c.htm](http://www.fas.org/irp/congress/1998_hr/s980224c.htm)> accessed November 2016.

<sup>372</sup> Trading with the Enemy Act of 1917 (40 Stat. 411) 12 U.S.C. Subchapter IV §95a.

<sup>373</sup> Trading with the Enemy Act of 1917 (40 Stat. 411) 12 U.S.C. §95a(A); Folendorf, C.L. *Breaking Terror's Bank without Breaking the Law: A comment on the USA PATRIOT Act and the United States War Against Terrorism* (2003-2004) 23 Journal of National Association of Administrative Law Judges 481, 484.

<sup>374</sup> *ibid* Folendorf.

NB. Amended in 1933 to widen scope to include national emergencies outside times of war, then amended again in 1970s to narrow scope back to times of war with introduction of the International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35) to deal with emergencies outside times of war.

<sup>375</sup> Under §120005, Title XII Violent Crime Control and Law Enforcement Act of 1994 (Pub. L. 103-322, 108 Stat. 1796) (42 U.S.C. Ch. 136) <<http://www.gpo.gov/fdsys/pkg/BILLS-103hr3355enr/pdf/BILLS-103hr3355enr.pdf>> accessed November 2016, which introduced §2339A into Chapter 113A of Title 18, US Code.

<sup>376</sup> Under §1705 International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35) enabling punishment for whoever finances designated terrorist organisations under Presidential Orders with up to 20 years in prison and a fine. Gurulé, J. *Unfunding*

introduced Executive Order 12,947, which prohibited transactions with specific terrorist organisations which disrupted the Middle East Process,<sup>377</sup> including the HAMAS and Hezbollah groups.<sup>378</sup> Moreover, in 1998, after the US Embassy bombings in Kenya and Tanzania, Executive Order 13,099 was also introduced, extending the list of prohibited persons and groups to include Osama bin Laden and his terrorist organisation al-Qaeda.<sup>379</sup> Additionally, Executive Order 13,129 in 1999 specifically identified Afghanistan and its Taliban government as a “safe haven” for al-Qaeda and subsequently blocked any US transactions with the country.<sup>380</sup> Therefore, there was some form of undertaking towards targeting the finances of terrorists and their groups by the US through executive action. Additionally, the Orders generated some successes, including freezing \$34million of Taliban assets held in US financial institutions as well as \$215million in gold<sup>381</sup> although, as the 9/11 Commission subsequently claimed, this was ‘easily circumvented’ because there were no multi-jurisdictional instruments to ensure that other countries’ financial systems were not used to channel terrorist finances.<sup>382</sup>

---

*Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008), 278.

<sup>377</sup> Executive Order 12,497: *Prohibiting Transactions With Terrorists Who Threaten To Disrupt The Middle East Peace Process*, (23 January 1995); enacted under the International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35) <[www.archives.gov/federal-register/executive-orders/](http://www.archives.gov/federal-register/executive-orders/)> accessed November 2016.

<sup>378</sup> *ibid* 4.

<sup>379</sup> Executive Order 13,099: *Prohibiting Transactions With Terrorists Who Threaten To Disrupt The Middle East Process*, (20 August 1998) <[www.archives.gov/federal-register/executive-orders/](http://www.archives.gov/federal-register/executive-orders/)> accessed November 2016.

<sup>380</sup> Executive Order 13,129: *Blocking Property and Prohibiting Transactions With the Taliban*, (4 July 1999) <[www.archives.gov/federal-register/executive-orders/](http://www.archives.gov/federal-register/executive-orders/)> accessed November 2016.

<sup>381</sup> Due to Executive Order 13129; *9/11 Commission Report* (22 July 2004), 185 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>382</sup> *ibid*.

Although these Orders showed the potential for freezing and preventing the flow of terrorist finances into the US,<sup>383</sup> they were issued under the International Emergency Economic Powers Act of 1977.<sup>384</sup> For instance, under §1702(b), the Orders are only allowed to be “...exercised to deal with an unusual and extraordinary threat with respect to which a national emergency...”,<sup>385</sup> although it is for the President to determine and declare a national emergency in peacetime.<sup>386</sup> Furthermore, the asset freezing provisions under the Presidential Orders were temporary, consequently, the President could not permanently seize assets determined to finance terrorist acts against the US.<sup>387</sup> Therefore, the powers the President had with respect to CTF could only be used in a national emergency and were temporary rather than permanent. Furthermore, as the 9/11 Commission alleged, the Executive Order against al-Qaeda resulted in few assets being frozen because the Treasury Department’s Office of Foreign Asset Control had little information to work from,<sup>388</sup> therefore rendering it partially ineffective.<sup>389</sup>

Nevertheless, one piece of CTF legislation was passed in the wake of both the Oklahoma City bombings in 1996 and Clinton’s Presidential Order 12,947 – the Antiterrorism and Effective Death Penalty Act (AEDPA).<sup>390</sup> For instance, under §302,

---

<sup>383</sup> E.g. They were used to find out and block some of Osama Bin Laden’s sources of financing; *9/11 Commission Report* (22 July 2004), 185-186 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>384</sup> §1702 International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35) (hereinafter ‘IEEPA 1977’).

<sup>385</sup> IEEPA 1977 §1702(b).

<sup>386</sup> IEEPA 1977 §1701(a).

<sup>387</sup> *The International Emergency Economic Powers Act: A Congressional Attempt to control Presidential Emergency Power* (1983) 96 Harvard Law Review 1102, 1109.

<sup>388</sup> *9/11 Commission Report* (22 July 2004), Chapter 6, 185 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>389</sup> *9/11 Commission Report* (22 July 2004), Chapter 6 (fn79) <<http://www.9-11commission.gov/>> accessed November 2016, whereby it explains that the OFAC froze the assets of Salah Idris, the owner of the al Shifa facility bombed in response to the Embassy bombings.

<sup>390</sup> Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) (Pub L. 104-132, 110 Stat. 1214) (hereinafter known as the AEDPA).



material support to designated terrorist organisation was prohibited<sup>391</sup> and an offence punishable with a fine and prison sentence of up to ten years<sup>392</sup> financial institutions were required to report transactions which they knew were connected to such organisations,<sup>393</sup> subsequently upheld by US courts in cases such as *Humanitarian Law Project v Reno*.<sup>394</sup> Furthermore, the Clinton administration announced the creation of the Foreign Terrorist Asset Tracking Center (FTATC)<sup>395</sup> which had a \$100 million budget to track assets connected with terrorist finances.<sup>396</sup> Consequently, it is apparent that the US had made some moves towards CTF under Clinton's Presidency, however, as outlined below, neither money laundering nor terrorist financing were considered a priority for Congress and State Departments<sup>397</sup> to invest in or further legislate against during the first years of George W. Bush's Presidency.<sup>398</sup> Indeed, it is claimed that, by September 2001, the FTATC, although having the funds to track terrorist financing, had no staff and no space to work.<sup>399</sup> Clearly, this had profound consequences.

Despite the legislative basis for CTF, the US had signed the UN's International Convention for the Suppression of the Financing of Terrorism on 10<sup>th</sup> January 2000,

---

<sup>391</sup> §303 AEDPA, inserting §2339B(a) into Chapter 113B, Title 18 U.S.C. and updating §2339A of Title 18 U.S.C.

<sup>392</sup> *ibid* Title 18 U.S.C. §2339A(a).

<sup>393</sup> *ibid* §2339B(a)(2).

<sup>394</sup> *Humanitarian Law Project v. Reno* (1998) 9 F. Supp. 2d 1176 (C.D. Cal.) – allowed the material support of a third party but did not include “training”.

<sup>395</sup> In May 2000 – see Weiss, M.A. RL32539 *CRS Report for Congress - Terrorist Financing: Current Efforts and Policy Issues for Congress* (20 August 2004), 9 <<http://www.au.af.mil/au/awc/awcgate/crs/rl32539.pdf>> accessed June 2018.

<sup>396</sup> Budget agreed by Congress in October 2000; *ibid* Weiss.

<sup>397</sup> E.g. Treasury Department and Department of Justice.

<sup>398</sup> Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 *Arizona Journal of International and Comparative Law* 835, 857-858 ref “sluggishness” of Clinton-era anti-money laundering provisions in Congress pre-9/11.

<sup>399</sup> *ibid* Weiss, 10.

yet only ratified its provisions *after* September 11, 2001.<sup>400</sup> This suggested that the issue was not of urgent priority to the US until after it had experienced terrorist attacks of this scale on its own soil.<sup>401</sup> Due to several high profile white collar crime cases in the late 1990s, such as Republic New York Securities, concerning a Ponzi scheme,<sup>402</sup> and the Pillsbury Company, concerning insider trading,<sup>403</sup> this may provide an insight into the US focus on white collar crime above terrorist financing. Therefore, although the US had the ability, the resources and the legislative tools to tackle terrorist financing internationally, as robustly as it had money laundering, it had failed to properly focus on the financing of terrorist acts before 9/11,<sup>404</sup> with the Treasury Department “*not consider[ing] [it] important enough to mention in its national strategy for money laundering*”.<sup>405</sup> Finally, it was alleged that the Attorney General at the time, John Ashcroft, had denied an FBI request for \$50 million for counterterrorism as late as 10 September 2001,<sup>406</sup> as he had instead focused efforts into the ‘war on drugs’.<sup>407</sup> This

---

<sup>400</sup> US ratified on 26 June 2002; United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999) <[http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=XVIII-11&chapter=18&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en)> accessed November 2016.

<sup>401</sup> *9/11 Commission Report* (22 July 2004), 341 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>402</sup> Gilpeth, K. (New York Times, 18 December 2001) *Republic New York Pleads Guilty to Securities Fraud* <<http://www.nytimes.com/2001/12/18/business/republic-new-york-pleads-guilty-to-securities-fraud.html>> accessed November 2016.

<sup>403</sup> *United States v. O'Hagan* 521 U.S. 642, 655 (1997).

<sup>404</sup> E.g. Louis Freeh, Director of FBI from 1993-2001, requested more resources to prevent terrorist acts, but was not provided with this, little human resources placed on counterterrorism duty despite being “top priority”, plus lack of information sharing; *9/11 Commission Report* (22 July 2004), 76-80, 107 <<http://www.9-11commission.gov/>> accessed November 2016; also see Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*, 4-6 <[https://govinfo.library.unt.edu/911/staff\\_state-ments/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_state-ments/911_TerrFin_Monograph.pdf)> accessed June 2018.

<sup>405</sup> *ibid.* *9/11 Commission Report* (22 July 2004), 186 <<http://www.9-11commission.gov/>> accessed November 2016; Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 146.

<sup>406</sup> Whether this would also have affected counter-terrorist financing is debatable, however, see Washington Post *Ashcroft's Pre-9/11 Priorities scrutinised* (12 April 2004) <[http://www.washingtonpost.com/wp-dyn/articles/A6589-2004Apr12\\_2.html](http://www.washingtonpost.com/wp-dyn/articles/A6589-2004Apr12_2.html)> accessed November 2016.

<sup>407</sup> CNN (Transcript, 7 February 2001) *Larry King Live: John Ashcroft Discusses His New Job as Attorney General* <<http://edition.cnn.com/TRANSCRIPTS/0102/07/lkl.00.html>> accessed November 2016; Borger, J. (The Guardian, 5 August 2002) *Bush held up plan to hit Bin Laden* <<https://www.theguardian.com/world/2002/aug/05/afghanistan.usa1>> accessed November 2016.

was in contrast to the UK, which devoted considerable legislative effort to combat terrorist financing.

### **3.2.3. The United Kingdom**

The UK also had AML legislation which criminalised hiding the proceeds of crime, some of which pre-dated international action. For example, the Drug Trafficking Offences Act 1986 introduced confiscation orders for the illicit proceeds of drugs trafficking,<sup>408</sup> the offence of assisting someone to retain the benefits of such proceeds,<sup>409</sup> as well as an exemption from this offence through reporting<sup>410</sup> and the Criminal Justice Act 1988 widened the UK's AML laws to include the confiscation of profits from other predicate offences.<sup>411</sup> Consequently, the UK had begun to expand the remit of the Vienna Convention towards hiding the illicit proceeds of other crimes.

Furthermore, unlike the US and Saudi Arabia, the UK, as a member of the EU and a founding member of the Council of Europe, was also subject to further legislation and Conventions relating to AML.<sup>412</sup> After the UN introduced the Vienna Convention, the Council of Europe also enacted its Convention on Laundering, Search, Seizure and Confiscation from Proceeds of Crime,<sup>413</sup> requesting that Member States

---

<sup>408</sup> Drug Trafficking Offences Act 1986, c.32, s. 1; *R v Cuthbertson* [1981] 1 AC 470. Showing problems of the Misuse of Drugs Act 1971 c.38 when confiscating proceeds of crime; Cribb, N. *Tracing and confiscating the proceeds of crime* (2003) 11(2) Journal of Financial Crime 168, 173-174.

<sup>409</sup> *ibid* Drug Trafficking Offences Act 1986, c.32, s. 24.

<sup>410</sup> *ibid* s. 24(3).

<sup>411</sup> Part VI Criminal Justice Act 1988; Financial Action Task Force *Third Mutual Evaluation report on Anti Money Laundering and Combating the Financing of Terrorism: The United Kingdom of Great Britain and Northern Ireland* (29 June 2007), 36 <<http://www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationoftheunitedkingdom-follow-upreport.html>> accessed April 2018.

<sup>412</sup> For EU measures, see section 3.2.1. *supra*.

<sup>413</sup> European Treaty Series No. 141 Convention on Laundering, Search, Seizure and Confiscation from Proceeds of Crime (8 November 1990) <<http://conventions.coe.int/Treaty/en/Trea->

enact AML.<sup>414</sup> This again widened the scope of AML to other forms of crime<sup>415</sup> including terrorist offences,<sup>416</sup> and containing “*an implicit invitation for such legislation to be as broad in scope as possible*”.<sup>417</sup> Furthermore, in 1993, the UK introduced the Criminal Justice Act, which built on previous legislation and the EU Money Laundering Directive<sup>418</sup> under Part III, and weakened the standard of proof for authorities from the criminal standard of beyond reasonable doubt to the civil standard of the balance of probabilities.<sup>419</sup> Moreover, the Money Laundering Regulations 1993 extended identification procedures to all financial institutions, including money services businesses.<sup>420</sup> Accordingly, it is evident that the UK had a broader set of AML regulations than set out in the Vienna Convention, enabling it to investigate and confiscate the proceeds of illegal acts.<sup>421</sup>

---

[ties/Html/141.htm](http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=141&CM=8&DF=23/10/2010&CL=ENG)> accessed November 2016; UK signed in 1990 and ratified in 1992 <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=141&CM=8&DF=23/10/2010&CL=ENG>> accessed November 2016.

<sup>414</sup> European Treaty Series No. 141 Convention on Laundering, Search, Seizure and Confiscation from Proceeds of Crime (8 November 1990), Article 2(1).

<sup>415</sup> *ibid* Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 St. Louis-Warsaw Transatlantic Law Journal 175, 187-188; Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 Tul. Journal Int'l & Comp. Law 161, 177-178; *ibid* Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129, 1134.

<sup>416</sup> Council of Europe Convention on the Laundering, Search, Seizure and Confiscation from Proceeds of Crime, Explanatory Note [8]; *ibid* Daley, M.J., 178; *ibid* Gilmore, W.C., 1135.

<sup>417</sup> *ibid* Gilmore, W.C., 1135.

<sup>418</sup> Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0308:EN:HTML>> accessed November 2016.

<sup>419</sup> Donohue, L.K. *Anti Terrorist Finance in the United Kingdom and the United States* (2005-2006) 27 Michigan Journal of International Law 303, 335.

<sup>420</sup> Money Laundering Regulations 1993 SI 1993/1933, Regulation 9; *ibid* Money Laundering Regulations 1993 Schedule, Note 2; Leong, 143.

<sup>421</sup> NB. Provisions reviewed after 9/11 under Part 7 of the Proceeds of Crime Act 2002, c.29 – e.g. no longer distinguishes between proceeds from drug trafficking and other criminal proceeds under s340 and provides three separate offences of money laundering under s327 (concealing, converting or transferring out of the UK criminal proceeds); Gentle, S. *Legislative Comment: Proceeds of Crime Act 2002* (2003) Compliance Officer Bulletin 12(Dec/Jan) 1-29; Money Laundering Regulations 2003 SI 2003/3075 and 2007; Snowden, P. and Lovegrove, S. *Money Laundering Regulations 2007* (2008) Compliance Officer Bulletin 54(Mar) 1.

### 3.2.3.1. The move towards counter-terrorist financing

Unlike the US,<sup>422</sup> the UK had long experience of terrorist attacks on its mainland before the events of 9/11 although, unlike 9/11 and its associated attacks, these were restricted by territory and politics. They were centred on the UK alone<sup>423</sup> and Irish nationalism, rather than against a particular ideology or lifestyle, which can encompass many countries.<sup>424</sup> With the emergence of Northern Irish terrorist organisations such as the Irish Republican Army (IRA), their need for economic resources to continue their operations and estimated running costs of between £500,000 and £1.5million per year,<sup>425</sup> the UK's legislation evolved to reflect the separate need to disrupt the flow of terrorist finances. For instance, the Prevention of Terrorism Act 1974 enabled the courts to forfeit assets which were "*controlled by an individual convicted of mem-*

---

<sup>422</sup> In comparison with the US, the UK has a broader and more detailed definition of terrorism and what constitutes a terrorist act under the Terrorism Act 2000 c.11 (e.g. it includes disruption of electronic systems under s. 1(2)(e)). Significantly, the definition of terrorism under s. 1 of the Terrorism Act expressly includes the "threat of action". This is different to the definition in U.S.C. Title 22, Ch.38, Paragraph 2656f(d), which does not include this wording. Interestingly, Lord Lloyd of Berwick, in his *Inquiry Into Legislation Against Terrorism* (1996), suggested that the definition of terrorism should be based upon the operational definition used by the FBI during the 1990s; Lord Carlile of Berriew *The Definition of Terrorism* Cm 7052 (Home Office, March 2007), 3, para.9 <<https://www.gov.uk/government/publications/the-definition-of-terrorism-a-report-by-lord-carlile-of-berriew>> accessed April 2018.

<sup>423</sup> E.g. US Government did little to stem the flow of donations to NORaid, which provided assistance to the Paramilitary IRA until 1980s; Levi, M. *Combating the Financing of Terrorism: A History and Assessment of the Control of Threat Finance* (2010) 50(4) British Journal of Criminology 650, 652 (fn 3); Donohue, L.K. (2005-2006) 27 *Michigan Journal of International Law* 303, 322-323; Donohue also explains that NORaid donated more than 50% of the resources needed by Paramilitary IRA for its armed campaigns - Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 123.

<sup>424</sup> For a good comparison between the IRA's and al-Qaeda's aims and objectives, see Greer, S. *Human Rights and the Struggle Against Terrorism in the United Kingdom* (2008) 2 European Human Rights Law Review 163, 165-167 (although the overall aim of the article relates to human rights and the treatment of terrorist suspects).

NB. IRA terrorism similar to Basque Separatist Group ETA (Euskadi Ta Askatasuna), which wanted a separate Basque region and concentrated attacks on the Spanish mainland and territories, European Union *EU List of Terrorist Organisations* (Council Common Position 2006/380/CFSP, 29 May 2006) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006E0380>> accessed April 2018.

<sup>425</sup> Donohue, L.K. *Anti Terrorist Finance in the United Kingdom and the United States* (2005-2006). 27 *Michigan Journal of International Law* 303, 324; 314-324 regarding different sources of funding.

bership, where such resources were intended for use in Northern Ireland terrorism".<sup>426</sup> Furthermore, the Prevention of Terrorism (Temporary Provisions) Act 1989 introduced specific provisions under Part III to criminalise the financing of terrorism<sup>427</sup> and the control of terrorist finances<sup>428</sup> as well as imposing forfeiture and criminal penalties on those found guilty of this offence.<sup>429</sup> Moreover, the Criminal Justice Act 1993 added separate provisions to counteract terrorist financing under Part IV,<sup>430</sup> lowering the standard of proof from criminal to civil standards,<sup>431</sup> and bringing it into line with AML legislation. After the Omagh bombings in 1998, the Criminal Justice (Terrorism and Conspiracy) Act 1998 also allowed courts to forfeit any property connected with proscribed terrorist organisations.<sup>432</sup> Therefore, it is evident that the UK already had a robust attitude towards disrupting terrorist finances and recognised it as a separate offence to money laundering, even before international action on the issue.

The UK was also one of the few countries to sign and ratify the provisions of the 1999 UN Convention on the Suppression of the Financing of Terrorism before 9/11.<sup>433</sup> Furthermore, the CTF provisions used by the UK government since 1975 were criticised on the basis that it did not extend provisions to terrorist acts committed anywhere abroad,<sup>434</sup> perhaps reflecting the point that previous legislation was centred

---

<sup>426</sup> *ibid* Donohue, 330.

NB. The Prevention of Terrorism Act had forfeiture provisions added in 1976.

<sup>427</sup> Prevention of Terrorism (Temporary Provisions) Act 1989, c.4 (repealed) s. 9 on contributions; *ibid* Donohue, 331-333; Cribb, N. *Tracing and confiscating the proceeds of crime* (2003) 11(2) *Journal of Financial Crime* 168, 177-178.

<sup>428</sup> *ibid* Prevention of Terrorism (Temporary Provisions) Act 1989, c.4 (repealed) s. 11.

<sup>429</sup> *ibid* s. 13.

<sup>430</sup> As amendments to the Northern Ireland (Emergency Provisions) Act 1991, c.24.

<sup>431</sup> Criminal Justice Act 1993 c.36, s. 37(2); Donohue, 336.

<sup>432</sup> Criminal Justice (Terrorism and Conspiracy) Act 1998 c.40, s. 4(3); Donohue 337-338.

<sup>433</sup> UN Convention on the Suppression of the Financing of Terrorism 1999. The UK signed 10 January 2000, ratified 7 March 2001; United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999) <[http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtidsg\\_no=XVIII-11&chapter=18&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtidsg_no=XVIII-11&chapter=18&lang=en). Botswana, Sri Lanka and Uzbekistan were the other countries who signed and ratified before 9/11.> accessed November 2016.

<sup>434</sup> Home Office *Legislation Against Terrorism* Cm4178 (HMSO, December 1998), Chapter 6

on terrorist acts in Northern Ireland and the UK, and had no mechanism to seize suspected terrorist finances while an investigation was ongoing.<sup>435</sup> The subsequent legislation, the Terrorism Act 2000 was, and still is, the cornerstone of the UK's CTF strategy through Part III of the Act. Significantly, the Act refined the definition of terrorism under the Prevention of Terrorism (Temporary Provisions) Act 1989,<sup>436</sup> and extended provisions relating to terrorism to include international terrorism and persons residing outside the UK.<sup>437</sup> The provisions included offences of fund-raising<sup>438</sup> and money laundering as part of concealing terrorist property,<sup>439</sup> confiscation and seizure of cash during an investigation<sup>440</sup> and penalties of forfeiture if convicted.<sup>441</sup> Accordingly, the UK was one of the few countries with properly separated CTF legislation and was most advanced in the application of financial weapons against terrorist organisations.<sup>442</sup> However, as will be outlined below, it is also evident that a number of UN Member States were not as advanced as the UK, creating problems with international co-operation before terrorism finally went global on September 11 2001.

---

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/265689/4178.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265689/4178.pdf)> accessed April 2018.

<sup>435</sup> *ibid.*

<sup>436</sup> Under the Prevention of Terrorism (Temporary Provisions) Act 1989, c.4 s. 20(1)(c), terrorism was defined as: "... *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*". This was found to be too broad by Lord Lloyd in his report on terrorism in 1996, therefore the words "serious violence" were inserted to refine it, as well as broader aspects being introduced to the definition, including 'threat of action' and application to religious and non-ideological groups; *ibid* Lord Carlile of Berriew *Definition of Terrorism*, 3, paras. 7-8.

<sup>437</sup> Terrorism Act 2000 c.11, s. 1(4)(a),(c) and (d).

<sup>438</sup> Terrorism Act 2000 c.11, s. 15.

<sup>439</sup> Terrorism Act 2000 c.11, s. 18.

<sup>440</sup> Terrorism Act 2000 c.11, s. 24-26.

<sup>441</sup> Terrorism Act 2000 c.11, s. 23.

<sup>442</sup> NB. The UK's anti-terrorist financing laws have been updated on a number of occasions since 9/11, for example, the Anti-terrorism, Crime and Security Act 2001 c.24, the Prevention of Terrorism Act 2005 c.2, the Terrorism Act 2006 c.11 and the Counter Terrorism Act 2008 c.28, as well as subsequent law enacted since the case of *A v HM Treasury* [2010] UKSC 2 which criticised the UK's Terrorism (United Nations Measures) Order 2006 SI 2006/2657 as being *ultra vires* by going far beyond the remit of the UN's original purpose of freezing orders, resulting in the Terrorist Asset-Freezing (Temporary Provisions) Act 2010 c.2, and Terrorist Asset-Freezing etc. Act 2010 c.38.

### 3.2.4. Kingdom of Saudi Arabia

Unlike legal systems in the UK and the US, which rely on common and blackletter law to penalise criminal activities and money laundering, Saudi Arabia on the other hand is a country which relies on the application of Shari'ah law against criminal conduct,<sup>443</sup> based on texts of the Islamic Holy Book, the Qur'an, as well as its interpretation by clerics.<sup>444</sup> As mentioned in the FATF Mutual Evaluation Report, published in June 2010, Shari'ah law already criminalised the collection and acquiring of illegal finances under the Qur'an,<sup>445</sup> based on a principle that "*prohibits the dealing of monies that have been gained illegally...*".<sup>446</sup> This, the Saudi Government claimed, covered all predicate offences relating to money laundering<sup>447</sup> and highlighted some success in prosecuting money laundering-related cases before 9/11.<sup>448</sup> Furthermore, Saudi Arabia had previously implemented Suspicious Activity Reports from 1975 onwards to prevent bank secrecy<sup>449</sup> and the Saudi Arabian Monetary Authority had been established since 1952 to supervise commercial banks and ensure the soundness of the financial sector.<sup>450</sup> Consequently, this suggested a good foundation for authorities to

---

<sup>443</sup> MENAFATF *Mutual Evaluation Report on Saudi Arabia*, (25 June 2010), 15, para. 53; 16, para. 54 <[www.fatf-gafi.org](http://www.fatf-gafi.org)> accessed November 2016; Basic Law of 1992 Article 8.

NB. Criminal conduct relating to financial crime should be viewed in the same light as Western countries because Saudi Arabia is signatory to a number of UN Conventions on this issue, e.g. Vienna and Palermo Conventions.

<sup>444</sup> NB. Shari'ah is based on five principles laid down in Islamic holy texts regarding human acts – obligatory (*wajib*), recommended (*mandub*), permissible (*mubah*), reprehensible (*makruh*) and forbidden (*haram*). Legal qualities are found in two principle sources – the Qur'an, and the *sunnah*, or the oral traditions regarding the words and deeds of the Prophet Mohammed. Furthermore, there is the doctrine of *ijma*, or consensus, which means that any legal decision which has been agreed upon unanimously, at any time, is the correct conclusion, as well as *qiyas*, the analogical reasoning and determination of the legality of certain acts, even when they are not clearly defined in the Qur'an or the *sunnah*. Lombardi, C. *Islamic Law as a Source of Constitutional Law in Egypt: The Constitutionalization of the Sharia in Modern Arab States* (1998) 37(1) *Columbia Journal of Transnational Law* 81 – although this refers to Egypt specifically, this text provides a clear overview of Shari'ah law.

<sup>445</sup> See in-depth analysis of money laundering under Shari'ah law - MENAFATF *Mutual Evaluation Report on Saudi Arabia*, 17, para. 62; 276-277 <[www.fatf-gafi.org](http://www.fatf-gafi.org)> accessed November 2016.

<sup>446</sup> *ibid* 30, para. 120.

<sup>447</sup> *ibid* 32, para. 128.

<sup>448</sup> *ibid* 31, para. 121 (fn 29); *Attorney General v. X* 17/09/1419AH (4 January 1999).

<sup>449</sup> *ibid* MENAFATF *Mutual Evaluation Report on Saudi Arabia*, 51.

<sup>450</sup> Saudi Arabian Monetary Authority, <[www.sama.gov.sa](http://www.sama.gov.sa)> accessed November 2016.



prohibit the proceeds of crime, although it is unclear how effective this was before 9/11.

Moreover, Saudi Arabia had ratified the Vienna Convention in 1992,<sup>451</sup> showing some steps it made against money laundering before 9/11. For instance, it introduced a Permanent Committee on Combating Money Laundering in 1999.<sup>452</sup> However, it was not until 2003 that Saudi Arabia had criminalised money laundering in line with the Vienna and Palermo Conventions,<sup>453</sup> emphasising that there was not a complete legislative framework in relation to money laundering or financial crime, for example, it did not include asset freezing or confiscation. This was unlike the UK and the US, which both had complied with the Conventions through their legislation.<sup>454</sup>

#### **3.2.4.1. The move towards counter-terrorist financing:**

Theoretically, the financing of terrorism under Saudi's Shari'ah law was already criminalised before 9/11.<sup>455</sup> As the MENAFATF Mutual Evaluation Report explains, under Shari'ah law, the financing of terrorism is considered "*a window to terrorism*,

---

<sup>451</sup> Saudi Arabia ratified 9 January 1992:

<[http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtldsg\\_no=VI-19&chapter=6&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtldsg_no=VI-19&chapter=6&lang=en)> accessed November 2016.

<sup>452</sup> *ibid* MENAFATF *Mutual Evaluation Report on Saudi Arabia*, 27.

<sup>453</sup> Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003.

<sup>454</sup> NB. Although both the UK and the US complied with International Conventions and had their own AML legislation, it is worth noting that in its 2006 Mutual Evaluation Report, the US was rated as "compliant" with 12 out of Forty Financial Action Task Force Recommendations "largely compliant" with 22 Recommendations, "partially compliant" with 2 and "non-compliant" with 4 Recommendations; Financial Action Task Force *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: The United States of America* (23 June 2006), 299, 302 <<http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf>> accessed April 2018.

In its Mutual Evaluation Report in 2007, the United Kingdom was rated as "compliant" with 19 out of the Forty Recommendations, "largely compliant" with 9 Recommendations, "partially compliant" with 9 Recommendations and "non-compliant" with 3 Recommendations; Financial Action Task Force *Third Mutual Evaluation report on Anti Money Laundering and Combating the Financing of Terrorism: The United Kingdom of Great Britain and Northern Ireland* (29 June 2007), 283-287 <<http://www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationoftheunited-kingdom-follow-upreport.html>> accessed April 2018.

<sup>455</sup> *ibid* MENAFATF *Mutual Evaluation Report on Saudi Arabia*, 37, para. 148.

*inseparable from terrorism*".<sup>456</sup> Consequently, a person who has contributed financially to a terrorist act could still be prosecuted, even if the act did not occur.<sup>457</sup> However, like the US, Saudi Arabia had not signed the 1999 UN Convention on the Suppression of Financing of Terrorism until after 9/11<sup>458</sup> and had not ratified its provisions until 2007,<sup>459</sup> highlighting that again, there was no complete framework in place to track financial transactions which could be used to finance terrorism. Furthermore, as the 9/11 Commission Report subsequently alleged, although the Saudi Arabian Government was assisting the US in counterterrorism efforts against al-Qaeda,<sup>460</sup> a network of terrorist financiers emerged in Saudi Arabia which contributed to al-Qaeda, known as the "Golden Chain".<sup>461</sup> A Joint Report by the US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence in 2002,<sup>462</sup> declassified in 2016,<sup>463</sup> shows allegations of specific individuals in the Saudi Government who had financed and assisted the operation. Accordingly, Saudi Arabia was vulnerable to the abuse of its banking system by terrorist financiers prior to 9/11, despite some of its regulations to prohibit financial crime.

---

<sup>456</sup> *ibid* 37, para. 148.

<sup>457</sup> *ibid* 38, para. 148.

<sup>458</sup> Saudi Arabia signed 21 November 2001; United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999)

<[http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=XVIII-11&chapter=18&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en)> accessed November 2016.

<sup>459</sup> Saudi Arabia ratified 23 August 2007; United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999)

<[http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg\\_no=XVIII-11&chapter=18&lang=en](http://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&lang=en)> accessed November 2016.

<sup>460</sup> *9/11 Commission Report* (22 July 2004), 123 <<http://www.9-11commission.gov/>> accessed November 2016, regarding pressurising Pakistan against the Taliban and Osama Bin Laden.

<sup>461</sup> *ibid* *9/11 Commission Report* (22 July 2004), 55, 170 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>462</sup> US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence *Joint Inquiry into Intelligence Community activities before and after the terrorist attacks of September 11, 2001* (December 2002), 415 <[https://fas.org/irp/congress/2002\\_rpt/911rept.pdf](https://fas.org/irp/congress/2002_rpt/911rept.pdf)> accessed June 2018.

<sup>463</sup> Smith, D. & Ackerman, S. (The Guardian, 15 July 2016) *9/11 report's classified '28 pages' about potential Saudi Arabia ties released* <<https://www.theguardian.com/us-news/2016/jul/15/911-report-saudi-arabia-28-pages-released>> accessed November 2016. Link to the redacted documents are also available through this story.

As will be discussed in further depth in this thesis, as Saudi Arabia applies Shari'ah law, its citizens are also liable to pay the charitable tax of *zakat* under Pillar Three of the five pillars of the Qur'an.<sup>464</sup> For instance, it was estimated in 2002 that Saudi Arabia alone generated \$10billion a year in zakat duties,<sup>465</sup> therefore a large amount of finances are produced by legitimate donations to charities.<sup>466</sup> Some concerns have consequently been raised that zakat could be used to mask finances used for criminal activity, including terrorism.<sup>467</sup> The practice which, unlike Western practices of voluntarily giving to charity, mandatorily requires 2.5 per cent of income to be donated to charities, and can be provided in cash to local community leaders, or anonymously, with little documentation as to where it ends up.<sup>468</sup> Furthermore, it has been claimed that some banks kept zakat donations out of their records, which meant that they could be potentially used for illegitimate purposes.<sup>469</sup> As the 9/11 Commission Report further states, charitable giving was subject to "limited oversight",<sup>470</sup> for

---

<sup>464</sup> E.g. Officially recognised in Saudi Arabia with the *General Authority for Zakat and Tax* <<https://www.gazt.gov.sa/en>>; Raphaeli, N. *Financing of Terrorism: Sources, Methods and Channels* (2003) 15(4) *Terrorism and Political Violence* 59, 61-62.

<sup>465</sup> Brisard, J.C. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing – Report Prepared for the President of the UN Security Council* (Investigative Project, 19 December 2002), 15 <<http://www.investigativeproject.org/documents/testimony/22.pdf>> accessed November 2016.

NB. Jean Charles Brisard has been subject to a number of defamation lawsuits regarding his report, e.g. *bin Mahfouz v Jean-Charles Brisard* [2006] EWHC 1191 (QB), *Al-Amoudi v Brisard* [2007] 1WLR 113.

<sup>466</sup> NB. Zakat is also used as a form of income tax for Saudi nationals (for non-Saudi nationals and companies, there are separate income tax laws).; General Authority of Zakat Tax <<https://www.gazt.gov.sa/en>> accessed April 2018.

<sup>467</sup> Raphaeli, N. *Financing of Terrorism: Sources, Methods and Channels* (2003) 15(4) *Terrorism and Political Violence* 59, 62.

<sup>468</sup> Council on Foreign Relations *Task Force Report Terrorist Financing* (2002), 7 <<http://www.cfr.org/economics/terrorist-financing/p5080>> accessed November 2016.

NB. This report was criticised by both the Saudi Government and the US Treasury Department, therefore updated in 2004 and tough Saudi Arabian laws regarding charitable oversight were introduced in 2003 and 2008.

<sup>469</sup> *ibid* Raphaeli, N. *Financing of Terrorism: Sources, Methods and Channels* (2003) 15(4) *Terrorism and Political Violence* 59, 72.

<sup>470</sup> *ibid* 9/11 Commission Report (22 July 2004), 171, 372 <<http://www.9-11commission.gov/>> accessed November 2016.

example, sparse auditing of charities,<sup>471</sup> providing the 9/11 terrorists with an opportunity to siphon off funds to further their own ends. For instance, as Levitt and the 9/11 Commission state, al-Qaeda and Osama Bin Laden had links with both Saudi zakat and charitable organisations<sup>472</sup> such as the Al-Haramain Islamic Foundation.<sup>473</sup> Consequently, concerns were raised about the Saudi CTF strategy prior to 9/11, in particular, regarding the regulation of charities.<sup>474</sup>

Furthermore, Saudi Arabia has a popular and legal banking option which rests outside formal financial institutions and had been identified as a potential conduit for money laundering and terrorist financing after 9/11.<sup>475</sup> This was through informal value transfer systems, often referred to as *hawala*<sup>476</sup> and defined by Passas as “not

---

<sup>471</sup> Council on Foreign Relations *Task Force Report Terrorist Financing* (2002), 7 <<http://www.cfr.org/economics/terrorist-financing/p5080>> accessed November 2016.

<sup>472</sup> Levitt, M. *The Political Economy of Middle East Terrorism* (December 2002) Middle East Review of International Affairs, Volume 6 No. 4, 10; \$1-2 million per month given to al-Qaeda; 9/11 Commission Report (22 July 2004), 372 <<http://www.9-11commission.gov/>> accessed November 2016. NB. this will be discussed in more depth later in the thesis.

<sup>473</sup> *ibid* Levitt; 9/11 Commission Report (22 July 2004), Chapter 5, 170-171 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>474</sup> NB. UK and US also had difficulty regulating charitable donations to terrorist organisations – UK Charity Commission failed to investigate 8 charities with links to 2005 London bombings; Ryder, N. *Danger Money* (2007) New Law Journal 157(7300) Sup (Charities Appeals Supplement) 6, 8, 12. In the US, Benevolence International Foundation channelled funds to al-Qaeda using charitable status as a front (*United States v. Arnout* 02-CR-892 (N,D, III, 1 November 2002)) after gaining tax exempt status in 1993 from the Internal Revenue Service (IRS) – see Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 17.

<sup>475</sup> Ref. Money laundering, Passas N., *Informal Value Transfer Systems and Criminal Organisations: A Study into so-called Underground Banking Networks* (1999), 40 <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1327756](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327756)> accessed April 2018. Ref. Terrorist financing and hawala, see in general Pathak, R. *The Obstacles to regulating the hawala: A cultural norm or a terrorist hotbed?* (2003) 27 Fordham International Law Journal 2007, 2027 regarding 9/11 Commission Report identifying hawala funds being used for the attacks; Wheatley, J.A. *Ancient Banking, Modern Crimes: How Hawala secretly transfers the finances of criminals and thwarts existing laws* (2005) 26 University of Pennsylvania Journal of International Economic Law 347, 358 who contends it was not.

<sup>476</sup> Also known as hundi in India, fei'chen in China, phoe kuan in Thailand, and the Black Peso in South America; Wheatley, J.A. *Ancient Banking, Modern Crimes: How Hawala secretly transfers the finances of criminals and thwarts existing laws* (2005) 26 University of Pennsylvania Journal of International Economic Law 347, 348-349.

NB. The branding of informal value transfer systems as a whole with a general term like “hawala” by some Western scholars and governments is relatively inaccurate as it limits the practice to a few territories (i.e. the Middle East) and does not highlight how popular these forms of transfer are globally as well as how they differ from country to country (e.g. hawala is a bi-directional system of transfer – it can be transferred to persons in different countries and persons in different countries can transfer it

*involv[ing] traditional banking transactions or services... Instead, these are essentially mechanisms serving the transfer of value from place to place.*<sup>477</sup> Due to its lack of record-keeping and client confidentiality, hawala is said to be perfect for hiding and transferring criminal wealth,<sup>478</sup> as there is no paper trail for authorities to investigate. Most significantly, hawala is claimed to be a capable conduit for all three stages of money laundering,<sup>479</sup> “[eroding] *the dirty money trail, especially if the transactions cross borders...*”.<sup>480</sup> It is therefore suggested that informal value transfer systems were susceptible to secretly transferring criminal funds globally.

The hawala form of remittance is also extremely popular for legitimate transactions as it is much cheaper than formal banking transactions.<sup>481</sup> Overall, hawala generates around \$2trillion per annum globally.<sup>482</sup> Consequently, this makes it harder for law enforcement authorities to trace an illicit transaction underneath a plethora of legal transfers.<sup>483</sup>

---

home, whereas Chinese fei’chen transactions can only be transferred *into* China). This will be elaborated on later in the thesis but, for this section, as the term “hawala” is recognised throughout the Middle East and North Africa as the general name for their informal value transfer systems, it will be used. For a good study into different informal value transfer systems: Passas, N. *Informal Value Transfer Systems: A Study into so-called Underground Systems* (1999).

<sup>477</sup> *ibid* Passas, N., 1.

<sup>478</sup> *ibid* Wheatley, J.A., 356.

<sup>479</sup> Daudi, A. *The Invisible Bank: Regulating the Hawala System in India, Pakistan and the United Arab Emirates* (2005) 15 *Indiana International and Comparative Law Review* 619, 632-633.

<sup>480</sup> *ibid* Wheatley, J.A., 357.

<sup>481</sup> Perkel, W. *Money Laundering and Terrorism: Informal Value Transfer Systems* (2004) 41 *American Criminal Law Review* 183, 199.

<sup>482</sup> Ryder, N. *A False Sense of Security? An analysis of legislative approaches towards the prevention of terrorist finances in the United States and the United Kingdom* (2007) *Journal of Business Law* 821; Raphaeli, N. *Financing of Terrorism: Sources, Methods and Channels* (2003) 15(4) *Terrorism and Political Violence* 59, 70.

<sup>483</sup> The FATF in 2010 identified “cash intensive” jurisdictions as a threat to anti-money laundering and counter terrorist financing measures as illicit transactions can be “easily integrated” into the legal economy and large cash transactions are common; Financial Action Task Force *Global Money Laundering and Terrorist Financing Threat Assessment* (July 2010), 54 <<http://www.fatf-gafi.org/publications/methodsandtrends/documents/globalmoneylaunderingterroristfinancingthreatassessment.html>> accessed April 2018.

### 3.3. Technology

Terrorist organisations, such as al-Qaeda and the IRA use the Internet to finance their operations<sup>484</sup> because of three vital aspects of the Internet – it is cheap, fast and, on the whole, anonymous,<sup>485</sup> putting them at a significant advantage over law enforcement authorities, whose investigations are inevitably time-consuming, expensive and must cross multiple jurisdictions.<sup>486</sup> Additionally, with increasing reliance on digital banking and the rise of virtual currencies such as Bitcoin, these provide multiple resources for terrorists and criminals to exploit and evade capture.<sup>487</sup> As mentioned in chapter one, terrorists use the Internet to raise and channel finances in three ways:

- (i) Direct solicitation of donations, communicating through websites and emails
- (ii) Use of legitimate sources such as charities and financial institutions, and
- (iii) Online crime.

Consequently, the use of the Internet has become an extremely valuable source of raising and channelling finances efficiently and cheaply for terrorist organisations.

---

<sup>484</sup> E.g. the case of Babar Ahmad and al-Qaeda supporting website azzam.com which had links to solicit donations; Davis B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 141; Real-IRA used websites such as Amazon.com to raise finances for their operations; Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 285.

<sup>485</sup> Conway, M. *Terrorism and the Internet: Core Governance and Issues* (2007) 3 Disarmament Forum 23, 25.

<sup>486</sup> Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223, 142 – see their example of the “Love Bug” virus which illustrated the challenges law enforcement faced when investigating crimes conducted through the Internet, as the Philippines had no cybercrime law or penalties for hacking, therefore the prosecution against the virus’ disseminator failed, nor could he be extradited due to the US’s requirement of “double criminality” for cases of cybercrime, i.e. that there must be a crime in both countries in order for extradition to work (pp139-141); Rider, B. *Cyber-organised crime – the impact of information technology on organised crime* (2001) 8(4) Journal of Financial Crime 332, 341-342.

<sup>487</sup> Financial Action Task Force *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014) <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>> accessed November 2016.

Since the late 1980s and early 1990s, use of the Internet has exploded globally through the advent of personal computers and cheap Internet connection,<sup>488</sup> enabling many around the world to communicate internationally, as well as instantly transfer cash, either through formal financial institutions, or informally, through value transfer,<sup>489</sup> across a number of territorial borders. Moreover, the Internet opened up new possibilities of criminal enterprise through conducting traditional financial crimes over the Internet,<sup>490</sup> falling under the generic title of cybercrime.<sup>491</sup> It is worth noting here that the term “cybercrime” covers a wide area of criminal activities and can also be referred to, confusingly, by national jurisdictions and international organisations as “computer crime”,<sup>492</sup> as there is no internationally recognised definition. Brenner and Goodman define cybercrime as covering two types of offence – the first is that the computer is the target of the offence (through attacks on data integrity and network confidentiality by unauthorised access and tampering with data)<sup>493</sup> and the second being the conduct of traditional crimes such as fraud with the assistance of a computer or computer networks.<sup>494</sup> Furthermore, Wall divides types of cybercrime into three delineated areas:

---

<sup>488</sup> Adams, J. *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet* (1996) 12 Santa Clara Computer and High Tech Law Journal 403, 405; 407-408.

<sup>489</sup> E.g. e-Gold.

<sup>490</sup> E.g. Money laundering over the Internet (aka cyberlaundering); *ibid* Rider, B. *Cyber-organised crime – the impact of information technology on organised crime* (2001) 8(4) Journal of Financial Crime 332, 335 – computers enable complex transactions to hide criminal wealth easily; fraud such as credit card fraud; *ibid* Rider, B., 338-339; “phishing” emails, building on traditional confidence trickster letters, to random email addresses to gain cash, *ibid* Rider, B.

<sup>491</sup> NB. Cybercrime is not just financial crime conducted over the Internet – the Federal Bureau of Investigation has defined four subheadings under cybercrime – (i) cybercrime against children, (ii) theft of intellectual property (iii) publication and intentional dissemination of malware (e.g. viruses) and (iv) national and international Internet fraud. Federal Bureau of Investigation Cybercrime Division *Key Priorities* <<http://www.fbi.gov/about-us/investigate/cyber/cyber>> accessed November 2016.

<sup>492</sup> NB. Use of these terms can also include physical offences against a computer, integrity of data systems, programmes and data itself, especially during the 1980s and early 1990s.

<sup>493</sup> Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223, 144.

<sup>494</sup> *ibid*.

- (a) *Crimes against machines/Integrity related* (e.g. hacking, sending viruses, spam emails);
- (b) *Crimes using machines/Computer related* (e.g. credit card fraud, identity theft, phishing, intellectual property theft) and,
- (c) *Crimes in the machine/Content related* (e.g. stalking, harassment, pornography, paedophilia, targeted hate speech and discussing drugs or bombs).<sup>495</sup>

Unlike many traditional crimes, cybercrime can be international by nature, with communications and illicit finances travelling through a number of Internet Service Providers based in different countries.<sup>496</sup> Furthermore, economic cybercrime is extremely lucrative, generating an estimated \$100billion globally per year by 2007,<sup>497</sup> quadrupling to \$400billion by 2014.<sup>498</sup> By comparison, it is estimated that the overall cost of cybercrime to companies by 2019 will be \$2trillion.<sup>499</sup> Therefore, law enforcement must have information- and evidence-sharing between countries, as well as similar legislative instruments, to be able to track the crime and prosecute the perpetrators.

Prior to 9/11, many domestic and international authorities focused on the issue of explicit criminal use of the Internet,<sup>500</sup> rather than using the Internet to channel ei-

---

<sup>495</sup> Wall, D. *The Internet as a conduit for criminal activity* (2005) 77-98 (Pattavina, A. (ed) *Information Technology and the Criminal Justice System* Thousand Oaks CA: Sage. Chapter revised March 2010), 4.

<sup>496</sup> Fletcher, N. *Challenges for regulating financial fraud in cyberspace* (2007) 14(2) *Journal of Financial Crime* 190, 198 (regarding jurisdiction).

<sup>497</sup> International Telecommunications Union *Understanding Cybercrime: A Guide for Developing Countries* (2009), 11 <<https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cyber-crime-guide.pdf>> accessed April 2018.

<sup>498</sup> McAfee Internet Security *Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II* (June 2014), 1:<<https://www.csis.org/events/2014-mcafee-report-global-cost-cybercrime>> accessed April 2018.

<sup>499</sup> Morgan, S. *Cyber Crime Costs Projected To Reach \$2 Trillion by 2019* (Forbes, 17 January 2016) <<http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#118419f23bb0>> accessed November 2016.

<sup>500</sup> See in general about types of cybercrime Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) *International Journal of Law and Information Technology* 139-223, 146-151.



ther illicit or legitimate finances for an illegal purpose. Consequently, the investigation and prevention of terrorist finances over the Internet faced significant international challenges, and also needed the intervention and guidance of international organisations such as the UN. The UN, however, has been traditionally detached when making recommendations on Internet regulation, leaving much of this issue up to domestic authorities.<sup>501</sup>

### **3.3.1. The United Nations and other International Organisations**

#### **3.3.1.1. Direct solicitation of donations**

The main use of the Internet by terrorists to finance their operations is through the direct solicitation of funds.<sup>502</sup> As Hinnen states, this includes direct appeals through websites with terrorist sympathies,<sup>503</sup> communication through chat rooms<sup>504</sup> and mass e-mailings to potential donors.<sup>505</sup> In order to counteract these ways of financing future operations, surveillance of websites and interception of e-mails are often

---

<sup>501</sup> Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 11 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016; Davis B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 164; UN Charter 1945 which provides discretion on UN intervention in matters (Article 1 for purposes of the UN and Article 2(7) ensuring that the UN is unable to intervene in matters falling under domestic jurisdiction. NB. The UN may be able to implement controls over the Internet through Article 1(3) on international co-operation on economic or cultural issues.

<sup>502</sup> Lewis, J.A. *The Internet and Terrorism* (2005) 99 Am. Socy Intl. L Proc 112, 112.

<sup>503</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 9.

<sup>504</sup> *ibid*; Lewis, J.A., 112.

<sup>505</sup> *ibid* Hinnen; Tibbetts, Lt. Col. P. S. *Terrorist Use of the Internet and Related Information Technology: A Monograph* School of Advanced Military Studies, Fort Leavenworth (2001-2002), 19 <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.859.2001&rep=rep1&type=pdf>> accessed June 2018; Lewis, J. A. *The Internet and Terrorism* (2005) 99 Am. Socy Intl. L Proc 112, 112.

deemed necessary by national governments.<sup>506</sup> Before 9/11, the UN distanced itself from an overall control of communications surveillance, leaving it up to sovereign jurisdictions to decide the level of surveillance they needed as an “*ad hoc endeavor*”.<sup>507</sup> There was little international regulation over the transmission of information over the Internet or of what information was being transmitted,<sup>508</sup> rather, the Internet was viewed as an open, decentralised network.<sup>509</sup> This ethic was bolstered by the interpretation of the Universal Declaration of Human Rights, which provides freedom to impart information through media communications,<sup>510</sup> while allowing exceptions for sovereign jurisdictions’ law enforcement agencies to intercept communications.<sup>511</sup> Consequently, the UN did, and still does, leave website and email communication surveillance to individual Member States to carry out and other international organisations to provide guidelines on, such as the EU.

Similarly, the EU concentrated on providing guidelines for the protection of

---

<sup>506</sup> Whitehouse Archives *Safeguarding America: President Bush signs PATRIOT Act Reauthorisation* (9 March 2006) <<https://www.justice.gov/archive/opa/docs/patriotact03-09-06.pdf>> accessed April 2018.

<sup>507</sup> Davis B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 161.

<sup>508</sup> Whitton, M. *Progression and Technological Advancement of Terrorist Financing: Are current laws adequate?* (2005).

<sup>509</sup> Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223; E.g. Internet Corporation of Assigned Names and Numbers (ICANN) is one of the only international bodies which monitor the use of the Internet through assigning domain names – this is a decentralised non-profit organisation, although it is based in the U.S.

<sup>510</sup> Article 19, Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A); Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 53 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016.

<sup>511</sup> *ibid* Article 27(2); *ibid* Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016.

personal data through the European Council introducing the 1995 Data Protection Directive,<sup>512</sup> stating that “*Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*”.<sup>513</sup> As a result, before 9/11, the EU’s main focus was on data protection policy rather than providing guidelines on surveillance or combating terrorist communications and solicitation of donations via this medium.<sup>514</sup>

### 3.3.1.2. Use of legitimate sources

As mentioned previously, online transactions are an ideal means of transferring money quickly, conveniently and globally.<sup>515</sup> For instance, the efficiency e-banking provides for the majority of Internet users<sup>516</sup> make it attractive to those who channel finances eventually used for terrorist activities.<sup>517</sup> Before 9/11, the UN used the implementation of the 1999 International Convention for the Suppression of the Financing of Terrorism to set international levels on preventing the use of financial institutions by

---

<sup>512</sup> *ibid* Commission Communication; Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 97/66/EC (15 December 1997) concerning the processing of personal data and the protection of privacy in the telecommunications sector on protecting privacy in the telecommunications sector, and Convention for the Protection of Human Rights and Fundamental Freedoms 1950 Article 8(1) on privacy in correspondence.

<sup>513</sup> *ibid* Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 1(1).

<sup>514</sup> NB. The Treaty of Lisbon 2009, replacing the European Union’s founding Treaty of Rome 1957, and which binds Member States explains at Article 6 that Member States are to recognise the Charter of Fundamental Rights of the European Union 2000/C 364/01 (7 December 2000 – amended in 2007) – this strengthens respect for a private life including communications under Article 7 and data protection under Article 8.

<sup>515</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 28.

<sup>516</sup> US Department of the Treasury *U.S. National Money Laundering Strategy 2007* (i) <<https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf>> accessed April 2018.

<sup>517</sup> *ibid*.

terrorists through the Internet. Under Article 18 of the UN Convention, financial institutions are required to file suspicious activity reports<sup>518</sup> to FIUs or relevant government agencies,<sup>519</sup> and to promote customer identification<sup>520</sup> in order to combat terrorist financing. However, it is unclear whether these applied to Internet transactions, therefore it was likely that it was left to individual financial institutions and domestic authorities to implement these measures to Internet banking. Nevertheless, as Hinnen notes, these requirements are nearly impossible for financial institutions to carry out without face-to-face banking, although risks are reduced by requiring identification<sup>521</sup> for new customers.<sup>522</sup> Consequently, the provisions outlined by the UN to prevent terrorist financing through legitimate sources may not have been popularly implemented with online banking prior to 9/11.<sup>523</sup>

### 3.3.1.3. Cybercrime

---

<sup>518</sup> 1999 Convention, Article 18(1)(b)(iii). N.B. Article 18 also applies to charitable organisations.

<sup>519</sup> NB. Here, ‘relevant governmental agencies’ mean those financial crime units which are not recognised as Financial Intelligence Units (FIUs) or members of the Egmont Group of Financial Intelligence Units. According to the Egmont Group, there are four types of FIU: (i) Judicial (received by investigatory authorities to enable judicial powers to be enforced, e.g. asset freezing, seizing funds) (ii) Law Enforcement (supporting law enforcement authorities during their investigations) (iii) Administrative (independent, administrative body which disseminates and discloses information from financial institutions to judiciary or law enforcement authorities) and (iv) Hybrid (incorporating at least two of the other models) Egmont Group *Financial Intelligence Units* <<https://egmont-group.org/en/content/financial-intelligence-units-fius>> accessed April 2018.

<sup>520</sup> 1999 Convention on the Suppression of Terrorism, Article 18(1)(b)(i) and (ii); Bantekas, I. *Current Developments: The International Law of Terrorist Financing* (2003) 97 *American Journal of International Law* 315, 325.

<sup>521</sup> E.g. Driving licence numbers and social security numbers in the U.S.

<sup>522</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5, 29.

<sup>523</sup> NB. The Basel Committee on Banking Supervision set up an Electronic Banking Group by the year 2000, which issued its Risk Management Principles for Electronic Banking in May 2001. This highlighted the need for identification measures at Principle 4 due to concerns about ID theft and money laundering, Basel Committee on Banking Supervision *Risk Management Principles for Electronic Banking*, 14 (May 2001) <<http://www.bis.org/publ/bcbs82.pdf>> accessed November 2016.

The advantages of the Internet to transfer money globally, such as speed and anonymity, work in favour of criminals using the Internet for illicit purposes, such as cyber-laundering. Electronic cash is “*not bulky and cumbersome like regular cash*”,<sup>524</sup> is anonymous through the ability to disguise a location<sup>525</sup> and has no uniform, regulated system of identification for e-transactions to financial institutions.<sup>526</sup> Consequently, the processes of placement, layering and integration are relatively simple and nearly untraceable because of the Internet’s global reach.<sup>527</sup> The advent of e-commerce has also become an ideal source of raising and channelling terrorist finances through illicit activities. For example, auction sites such as eBay and Yahoo! Auctions have links to terrorist financing through terrorist organisations selling items on them to raise cash.<sup>528</sup> Again, the anonymity of the Internet is an advantage to terrorist financiers as “*nobody need know exactly what goods or services changed hands or if, in fact, anything other than cash changed hands at all...*”.<sup>529</sup> Moreover, the use of credit card fraud and identity theft provide terrorist organisations with the ability to access bank accounts within domestic jurisdictions, bypassing bulk cash reporting requirements.<sup>530</sup> Furthermore, the use of fraudulent company and banking web pages and e-mails, or

---

<sup>524</sup> Baldwin, F.N. *The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?* (2004) 8(2) *Journal of Money Laundering Control* 127, 139.

<sup>525</sup> *ibid.*

<sup>526</sup> *ibid.*

<sup>527</sup> *ibid.* 140.

<sup>528</sup> Tibbetts, Lt Col P. S. *Terrorist Use of the Internet and Related Information Technology: A Monograph* School of Advanced Military Studies, Fort Leavenworth (2001-2002), 21-22  
<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.859.2001&rep=rep1&type=pdf>> accessed June 2018.

<sup>529</sup> *ibid.* 22.

<sup>530</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5, 22; Baldwin, 140.

phishing, allows terrorists to gain cash and personal information to finance their operations.<sup>531</sup>

However, during the 1990s, the UN concerned itself with offences which targeted computers themselves through maintaining data integrity.<sup>532</sup> For instance, in 1994, the UN issued a Manual on the Prevention and Control of Computer-Related Crimes, highlighting the vulnerabilities of global dependence on computers.<sup>533</sup> Furthermore, the Manual urged Member States to co-operate with each other and harmonise laws to combat the problem of computer-related crime.<sup>534</sup> However, the definitions used of “computer crime” did not necessarily include economic cybercrime through ID theft or credit card fraud. For example, the Manual only listed integrity and correctness of data stored on computers (e.g. the prevention of mischief and vandalism of data through viruses and hacking),<sup>535</sup> and the exclusive use of data (e.g. intellectual property and protection of trade secrets).<sup>536</sup> It is therefore ambiguous as to

---

<sup>531</sup> *ibid* Hinnen, 23; Smith, M., Seifert, J. McLoughlin, G. & Moteff, J. *Congressional Research Service Report to Congress The Internet and the USA PATRIOT Act: Potential Implications for Electronic Security, Commerce and Government* (4 March 2002) regarding identity theft, 15-18, <<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-004.pdf>> accessed April 2018.

<sup>532</sup> 8<sup>th</sup> UN Congress on the Prevention of Crime and the Treatment of Offenders introduced a resolution on the growing issue of “computer crime” in 1990 endorsed by UN Resolution A/RES/45/121 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (14 December 1990) <<http://www.un.org/documents/ga/res/45/a45r121.htm>> accessed November 2016; Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) *International Journal of Law and Information Technology* 139-223, 166-167; UN Resolution A/RES/52/91 Preparations for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (12 December 1997) and A/RES/53/110 Preparations for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (9 December 1998) calling for workshops on crimes related to the computer network (i.e. the Internet) at the 10<sup>th</sup> UN Congress on the Prevention of Crime and Treatment of Offenders – although these were to discuss the issue of cybercrime.

<sup>533</sup> UN Office on Drugs and Crime *UN Manual on the Prevention and Control of Computer Related Crimes 1994*, para. 4 <[https://www.unodc.org/pdf/Manual\\_ComputerRelatedCrime.PDF](https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF)> accessed April 2018.

<sup>534</sup> *ibid* paras. 116-126.

<sup>535</sup> *ibid* paras.90-95.

<sup>536</sup> *ibid* paras. 96-115.

whether these guidelines could have been used by individual jurisdictions to track illicit payments and credit card fraud.

Nevertheless, in 2000, the UN 10<sup>th</sup> Congress on the Prevention of Crime and Treatment of Offenders broadened its interpretation of the scope of computer crime to include cybercrime, outlining online phenomena such as phishing, as well as predicting that e-commerce would be vulnerable to fraud and cyber-laundering.<sup>537</sup> Consequently, in 2000 General Assembly Resolution A/RES/55/63 was introduced, noting of value the exchange of information between Member States of the pitfalls of investigations in this area,<sup>538</sup> as well as MLA,<sup>539</sup> although Member States were not required to implement these measures. Additionally, the lack of requirement to implement these measures, as Bell notes,<sup>540</sup> MLA agreements, which allow domestic law enforcement to investigate and prosecute cybercrime through information exchange with other countries, made investigations burdensome.<sup>541</sup> As a result, investigations may have been hampered by either the inadequacy of MLA or the shortcomings of domestic legislation relating to Internet crime.<sup>542</sup> Consequently, it was apparent before September 11, 2001 that, although concerned about cybercrime, the international commu-

---

<sup>537</sup> UN 10<sup>th</sup> Congress on the Prevention of Crime and Treatment of Offenders *Crime Fighting on the Net* (2000) <<https://www.un.org/press/en/2000/20000410.soccp216.doc.html>> accessed April 2018.

<sup>538</sup> *ibid* General Assembly Resolution A/RES/55/63 Combating the criminal misuse of information technologies (21 January 2001), s. 1(c).

NB. This invited rather than required Member States to comply at s. 2.

<sup>539</sup> *ibid* s. 1(g).

<sup>540</sup> Bell, R.E. *The prosecution of computer crime* (2002) 9(4) *Journal of Financial Crime* 308, 316-317.

<sup>541</sup> Due to their slow, expensive and complex nature; *ibid* 316.

<sup>542</sup> E.g. The “Love Bug” virus investigations resulted in no prosecution as the Philippines had no cybercrime law; Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) *International Journal of Law and Information Technology* 139-223, 140-141.

nity, through the UN, did not agree upon a comprehensive international legal instrument which enabled Member States to update their legislation and investigative tools to incorporate technological advances.

However, some international organisations also expressed their concern about the growing issue of cybercrime during the 1990s. For example, the G8 formed a Subgroup on Hi-Tech Crime in 1997,<sup>543</sup> stating that “*each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion*”.<sup>544</sup> This meant it was recommended that members update their laws to include abuse of computer networks (i.e. the Internet and telecommunications networks) and that data showing cybercrime (known here as high-tech crime)<sup>545</sup> should be retained and preserved so that law enforcement could access it quickly and ultimately use it as evidence in criminal proceedings. This culminated in the formation of 10 Principles by the Subgroup, including recommendations for MLA,<sup>546</sup> updated legal systems to permit data retention so law enforcement authorities could access evidentiary data for investigations<sup>547</sup> and to design telecommunications systems to

---

<sup>543</sup> *ibid* Brenner, S. & Goodman, M., 170; Bell, R.E. *The prosecution of computer crime* (2002) 9(4) *Journal of Financial Crime* 308, 310; US Department of Justice *Meeting of Justice and Interior Ministers of Eight Communiqué* (10 December 1997) <<https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf>> accessed April 2018; US Department of Justice *Statement by Attorney General Janet Reno on the Meeting of Justice and Interior Ministers of Eight* (10 December 1997) <<http://www.justice.gov/opa/pr/1997/December97/518cr.html>> accessed November 2016.

<sup>544</sup> *ibid* *Communiqué of Meeting of Justice and Interior Ministers of Eight*, 2.

<sup>545</sup> *ibid* 1-2 of the *Communiqué* which defines high-tech crime as: “*First, sophisticated criminals are targeting computer and telecommunications systems to obtain or alter valuable information without authority and may attempt to disrupt critical commercial and public systems. Second, criminals, including members of organized crime groups and terrorists, are using these new technologies to facilitate traditional offenses.*” This mirrors the definitions provided for cybercrime earlier in this chapter.

<sup>546</sup> US Department of Justice *G-8 Lyon Subgroup on Hi-Tech Crime: Communiqué* (10 December 2007), Principle VI <<https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf>> accessed April 2018.

<sup>547</sup> *ibid* Principle V.



help detect and prevent network abuse as well as to assist tracing of criminals and detection of evidence.<sup>548</sup> Consequently, it was clear that some international strategies were being developed to combat cybercrime during the 1990s.

Furthermore, the Organisation for Economic Cooperation and Development (OECD) issued its Guidelines for Consumer Protection in the context of e-commerce in 1999, recommending Governments and businesses to implement secure payment systems online<sup>549</sup> and fair business and advertising practices (limiting fraudulent advertising),<sup>550</sup> thereby highlighting some preventative measures to combat fraudulent activities over the Internet. Therefore, it is apparent that the issue of cybercrime and abuse of e-commerce to that end was of immediate concern to some international organisations and partnerships. However, as with money laundering, these were based on soft law, meaning that, without legally binding recommendations, many countries did not have to implement their guidelines and, as membership was not universal, often their reach would have been limited.<sup>551</sup> Therefore, it was up to individual jurisdictions, such as the US to implement their own legislative measures to combat the use of the Internet by terrorist organisations.

### **3.3.2. The United States**

---

<sup>548</sup> *ibid* Principle IX.

NB. There is also the 24/7 Network set up by the Subgroup, which provides technical assistance to collect and preserve data for distribution to other countries for criminal investigations and evidence collection. This is now used by 30 countries who have dedicated cybercrime units and capability for 24 hour assistance.

<sup>549</sup> OECD *OECD Guidelines for Consumer Protection in the context of e-commerce* (9 December 1999), Part V <<http://www.oecd.org/dataoecd/18/13/34023235.pdf>> accessed November 2016.

<sup>550</sup> *ibid* Part II.

<sup>551</sup> OECD has 34 members:

<[http://www.oecd.org/document/1/0,3343,en\\_2649\\_201185\\_1889402\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/1/0,3343,en_2649_201185_1889402_1_1_1_1,00.html)> accessed November 2016; G7 has seven members – United Kingdom, Germany, United States, France, Italy, Japan and Canada.

### **3.3.2.1. Direct solicitation of donations**

Before 9/11, the US had a number of surveillance measures contained within its legislation, for example, the Foreign Intelligence Surveillance Act of 1978 (FISA), which already allowed Government agencies such as the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) to monitor US-foreign communications during investigations of a criminal act.<sup>552</sup> However, these tended to be limited to conventional technologies, such as wiretapping telephone lines, rather than the use of the Internet by terrorist groups, which had already been noticed as early as the mid-1990s.<sup>553</sup>

Nevertheless, during the 1990s, partially prompted by the 1993 World Trade Center bombings, the US introduced the Communications Assistance for Law Enforcement Act of 1994,<sup>554</sup> which widened the scope of interception of telecommunications to include “electronic messaging services”.<sup>555</sup> Furthermore, the Act required telecommunications providers to assist law enforcement authorities in interception of

---

<sup>552</sup> Foreign Intelligence Surveillance Act of 1978 (Pub.L. 95–511, 92 Stat. 1783) (50 U.S.C. Ch. 36), §2511(2)(f), Title 18 U.S.C. Chapter 36.

<sup>553</sup> Davis B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 150-151.

<sup>554</sup> 47 U.S.C. §1001-1021; Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371, 376.

<sup>555</sup> Communications Assistance for Law Enforcement Authorities Act of 1994 (Pub. L. No. 103-414, 108 Stat. 4279) (47 USC 1001), §102(4).

electronic communications.<sup>556</sup> Despite these provisions, it is unclear whether the US was successful in their application before 9/11.<sup>557</sup>

With regard to communications within the US, the US focused on data privacy rather than surveillance measures. For instance, the First Amendment to the US Constitution protected freedom of speech, although this was balanced with national security requirements.<sup>558</sup> Regarding email communications, the privacy and warrant provisions of the Fourth Amendment of the US Constitution,<sup>559</sup> confirmed by the Supreme Court case of *Katz*,<sup>560</sup> carefully balanced the ability for surveillance in the name of national security with the privacy of US citizens, by ensuring that the courts had some ability to review surveillance requests through issuance of warrants. Moreover, Title III of the Omnibus Crime Control and Safe Streets Act 1968 clarifies the legalities of wiretaps on US citizens – i.e. they must be obtained by court order.<sup>561</sup> This ethic was bolstered by the Electronic Communications Privacy Act 1986 which also required court orders for electronic communications.<sup>562</sup> Consequently, it is clear that

---

<sup>556</sup> *ibid* Lee, L.T., 376; E.g. updating equipment and services to enable Government to intercept “all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber’s equipment, facility, or service, or at such later time as may be acceptable to the government” and to enable access to call-identifying information (§103, Communications Assistance for Law Enforcement Authorities Act of 1994 (Pub. L. No. 103-414, 108 Stat. 4279) (47 USC 1001)).

<sup>557</sup> Lee notes that it was subject to great criticism and limitations; Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371, 376-377.

<sup>558</sup> *Schenck v. United States* 249 U.S. 47 (1919); Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com* (2003) 1 JIJIS 88, 91.

<sup>559</sup> Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375, 379; *Olmstead v. United States* 277 U.S. 438 (1928).

<sup>560</sup> *United States v. Katz* 389 U.S. 347 (1967); *ibid* Mell, P., 384-5.

<sup>561</sup> Title III Omnibus Crime Control and Safe Streets Act 1968 §801(d) amending Part 1, Title 18 United States Code, Chapter 119.

<sup>562</sup> §2511 Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, 100 Stat. 1848) (18 U.S.C. 2701 et seq.).

most surveillance measures before 9/11 had to be properly balanced with court intervention, a contrast to provisions introduced after 9/11 under the USA PATRIOT Act.

Despite the balance between surveillance and data protection, as Davis notes, now-blacklisted organisations such as the Benevolence International Foundation openly solicited donations on their websites, which they were eventually channelling to terrorist organisations.<sup>563</sup> As Davis also mentions, despite knowledge of the Internet being used in this way, US authorities had failed to respond against the use of the Internet by terrorists before 2001.<sup>564</sup> Furthermore, although surveillance laws prior to 9/11 were balanced with privacy, it is argued that these measures prevented law enforcement authorities' ability to access e-mail communications without authorisation from the Attorney General,<sup>565</sup> causing investigations to be slow and burdensome. Consequently, although being aware of the use of the Internet by such organisations, the US and its legislation was limited to visibly criminal uses of computers and the Internet and concerns about cyber-attacks on the US information technology network<sup>566</sup> and that there was more focus on privacy requirements.

### **3.3.2.2. Use of legitimate sources**

As mentioned under 3.2.2, the US used the Bank Secrecy Act of 1970 to track illegitimate finances which were channelled through formal financial institutions through Currency Transaction Reports and customer identification. However, as outlined by

---

<sup>563</sup> Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 142-143; *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 17.

<sup>564</sup> *ibid* Davis, B.R., 150.

<sup>565</sup> E.g. Title III Omnibus Crime Control and Safe Streets Act 1968; §2516 Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, 100 Stat. 1848) (18 U.S.C. 2701 et seq.).

<sup>566</sup> *ibid* Davis, B.R., 123.

Hinnen,<sup>567</sup> it is unlikely that such institutions would have been able to apply the requirements of the Act to online banking.<sup>568</sup>

### 3.3.2.3. Cybercrime

The US had a battery of legislation directly aimed at the misuse of computers and the issue of cybercrime. For instance, the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,<sup>569</sup> criminalised improper access of computers used by Government and financial institutions.<sup>570</sup> However, this statute was limited as it focused on the authorisation of the user to access a computer rather than crimes when the criminal did not physically “access” the computer.<sup>571</sup> Consequently, the Computer Fraud and Abuse Act of 1986 was introduced, widening the scope of criminal offences to include theft of property via a computer through fraud<sup>572</sup> and the intentional damage or destroying data belonging to others.<sup>573</sup> Furthermore, the US responded to the growing use of the Internet and the issue of cybercrime by amending the Computer Fraud and Abuse Act in 1988, 1989, 1990 and 1994,<sup>574</sup> widening the scope of definitions to include all financial institutions when dealing with fraud and criminalising reckless acts of computer damage.<sup>575</sup> Moreover, with the increasing use of cyber-commerce and e-payment systems, which meant that cash was transferred electronically and

---

<sup>567</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 29.

<sup>568</sup> *ibid* Hinnen, (fn 307-308).

<sup>569</sup> Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Pub. L. 98-473, 98 Stat. 2190) 18 U.S.C. §1030.

<sup>570</sup> Jarrett, H.M. & Bailie, M.W. (US Justice Department, Computer Crime and Intellectual Property Section), 1 *Prosecuting Computer Crimes Manual, Chapter 1 “Computer Fraud and Abuse Act”* (Department of Justice, 14 January 2015) <<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>> accessed April 2018; Adams, 421.

<sup>571</sup> Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223, (fn 148); Adams, 422.

<sup>572</sup> *ibid* *Prosecuting Computer Crimes Manual*, 2; §1030(a)(4) U.S.C. Title 18; Adams, 423.

<sup>573</sup> *ibid*; §1030(a)(5)(A) U.S.C.; Adams, 423.

<sup>574</sup> Adams, 424-426.

<sup>575</sup> §1030(a)(5)(B) U.S.C Title 18; Adams, 425.

could be done so instantaneously and anonymously, the US government was aware of the possibilities of cyberlaundering.<sup>576</sup> Consequently, the US devised sting operations in cyberspace<sup>577</sup> and the Department of Justice created a Computer Crime and Intellectual Property Section in 1992<sup>578</sup> whose primary aim is “*implementing the Department's national strategies in combating computer and intellectual property crimes worldwide*”.<sup>579</sup> Additionally, the US Financial Crimes Enforcement Network (FinCEN), discussed the issue of cyberpayments and their vulnerability in cyberlaundering as early as 1995.<sup>580</sup> Therefore, it is evident that US legislation and law enforcement authorities were evolving to cope with the potential of using the Internet for criminal purposes as well as financial crime generated over the Internet.

However, despite legislation against cybercrime, it is clear that the US focused on acts which were, from the beginning, criminal by nature, a stance which does not catch all types of terrorist financing over the Internet. As Adams explains, crimes perpetrated over the Internet “*can be grouped into three major categories: 1) computer crimes 2) fraud and 3) noncomputer crimes...*”<sup>581</sup> As a result, computer crimes such as hacking and spreading viruses or worms over the Internet<sup>582</sup> were brought alongside classic non-computer crimes like fraud, distribution of child pornography

---

<sup>576</sup> Alexander, K. & Munroe, R. *Cyberpayments: internet and electronic money laundering – Countdown to the year 2000* (1996) 4(2) *Journal of Financial Crime* 156, 157.

<sup>577</sup> *ibid.*

<sup>578</sup> *ibid.*

<sup>579</sup> US Department of Justice *Computer Crime and Intellectual Property Section* <<https://www.justice.gov/criminal-ccips>> accessed April 2018.

<sup>580</sup> Alexander, K. & Munroe, R. *Cyberpayments: internet and electronic money laundering – Countdown to the year 2000* (1996) 4(2) *Journal of Financial Crime* 156, 158-160.

<sup>581</sup> Adams, 409.

<sup>582</sup> E.g. *United States v. Morris* 928 F.2d 504 (2d Cir. 1991); US Department of Justice Prosecuting Computer Crimes Manual, 6-8; Dierks, M. *Computer Network Abuse* (1993) 6 *Harvard Journal of Law and Technology* 307 (1992-1993), 317-319; Adams, 409-411; Loundy, D.J., *E-Law: Issues affecting computer information systems and systems operator liability* (1993) 3 *Albany Law Journal of Science and Technology* 79, 108-111 (viruses).

and copyright.<sup>583</sup> Moreover, the US attempted to prohibit online gambling in the late 1990s as some Congressmen were concerned about the legality of gambling websites<sup>584</sup> and the connection between online gambling and money laundering.<sup>585</sup> Consequently, the focus of US authorities was to prevent overtly criminal behaviour online. Nevertheless, movements towards prohibiting online gaming and preventing cybercrime would not have been sufficient for preventing terrorist groups from using the Internet to raise their finances, as they can be raised through legitimate means. By comparison, the UK relied on the use of its existing legislation to apply to online financial crime.

### **3.3.3. The United Kingdom**

#### **3.3.3.1. Direct solicitation of donations**

As mentioned earlier, the EU introduced the Data Protection Directive in 1995. This was applied in the UK's Data Protection Act 1998 which protected the privacy of personal data stored by computers<sup>586</sup> under the Data Protection Principles.<sup>587</sup> This included personal data being obtained "*only for one or more specified and lawful purposes*"<sup>588</sup> and prevented the transference of personal data to countries outside the European Economic Area unless they ensured "*an adequate level of protection for the*

---

<sup>583</sup> Adams, 413-414; Loundy, D. J. *E-law: Legal issues affecting computer information systems and systems operator liability* (1993) 3 Alb. L. J. Sci. & Tech. 79, 101-104 (child pornography); *ibid* Loundy, 124-132 (copyrighting).

<sup>584</sup> E.g. Internet Gaming Prohibition Act 1999 (defeated before Congress):

<<http://www.govtrack.us/congress/bill.xpd?bill=h106-3125>> accessed November 2016.

<sup>585</sup> FinCEN *A Survey of Electronic Cash, Electronic Banking and Internet Gaming* (2000), 51

<<https://www.fincen.gov/sites/default/files/shared/e-cash.pdf>> accessed June 2018; Mills, J. *Internet Casinos: A sure bet for money laundering* (2001) 8(4) *Journal of Financial Crime* 365.

<sup>586</sup> See Data Protection Act 1998 c.29 Part I s. 1(1)(a)-(c).

<sup>587</sup> *ibid* Schedule 1 Part I.

<sup>588</sup> *ibid* Schedule 1 Part I s. 2.

*rights and freedoms of data subjects*”.<sup>589</sup> As the EU’s main focus was on data protection rather than providing guidelines against cybercrime and online fraud this focus was therefore reflected in the UK’s own legislation.

However, despite European concentration on data protection, the UK had also begun to use surveillance on Internet communications to monitor crime before 9/11, going further than even the US in this area by providing legislation which would potentially catch solicitation of donations via email communications. Using data protection exemptions under the Data Protection Directive<sup>590</sup> and the Data Protection Act,<sup>591</sup> the main UK piece of legislation relating to Internet surveillance was the Regulation of Investigatory Powers Act (RIPA), introduced in 2000. This replaced the Interception of Communications Act 1985 (IOCA), which was deemed inadequate for Internet communications due to its narrow focus on only postal and telecommunications networks<sup>592</sup> and whose warrants only applied to one address – incompatible with numerous email addresses which individuals now use.<sup>593</sup>

Instead, RIPA can apply to two areas of Internet communications – the interception of messages (the content of an email), and the acquisition of data communications (data traffic such as the destination of an email, but no content<sup>594</sup>). Part I of

---

<sup>589</sup> *ibid* Schedule 1 Part I s. 8.

<sup>590</sup> Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 3(1) – the Directive does not apply for public security and investigation of criminal acts.

<sup>591</sup> Data Protection Act 1998 c.29 Part IV, s. 28 (national security) and s. 29(1)(a) and (b) (prevention and detection of criminal acts; apprehension and prosecution of offenders).

<sup>592</sup> Jabbour, V. *Interception of Communications - I: Private Rights and Public Policy* (1999) 15 Computer Law and Security Report 6, 390; Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 74-75.

<sup>593</sup> Sutter, G. *E-mail monitoring and interception 2001* (2001) 3 Electronic Business Law 2, 2, 2.

<sup>594</sup> Gillespie, A.A. *Regulation of Internet surveillance* (2009) European Human Rights Law Review 4, 552, 559.



RIPA deals with the interception of communications,<sup>595</sup> extending its remit and definitions to include Internet technology. Furthermore, s. 5 of the Act provides for lawful interception of communications with a warrant from the Home Secretary,<sup>596</sup> as long as it is necessary and proportionate,<sup>597</sup> and includes interceptions which are necessary in the interest of national security<sup>598</sup> or in the detection or prevention of a serious crime.<sup>599</sup> Moreover, the warrants can include email addresses<sup>600</sup> and communications providers are under a duty to assist in the interception of communications.<sup>601</sup> Additionally, RIPA warrants apply to the individual<sup>602</sup> rather than their address, catching concerns about narrow scope under the IOCA through including differing email addresses.<sup>603</sup> Under Part II, law enforcement authorities are able to track an individual's

---

<sup>595</sup> Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 74.

<sup>596</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(1); Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 77.

<sup>597</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(2).

<sup>598</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(3)(a) – although there is no universally recognised definition of “national security”, as the UK abides by Article 8 of the European Convention of Human Rights through the Human Rights Act 1998 c.42 (right to a private life unless in certain circumstances, including national security), it is worthwhile noting how the European Court of Human Rights interprets the national security exemption – i.e. whether it is proportionate to what is required in the running of a democratic society. In the case of 2EHRR 214 *Klass and others v The Federal Republic of Germany* (6 September 1978), the court explained at paragraph (i) that “as democratic societies found themselves threatened by highly sophisticated forms of espionage and by terrorism, the Court had to accept that legislation granting powers of secret surveillance over the mail etc of subversive elements within their jurisdiction was under exceptional conditions necessary in a democratic society in the interests of national security...”.

<sup>599</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(3)(b); definition of serious crime is outlined in s. 81(2)(b) under the tests in s. 81(3)(a) and (b) – (a) *that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one (eighteen in relation to England and Wales) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more; (b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.*

<sup>600</sup> Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 77; Regulation of Investigatory Powers Act 2000 c.23, s. 8(2).

<sup>601</sup> Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 78; Regulation of Investigatory Powers Act 2000 c.23, s. 11(4)(b) and (c).

<sup>602</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 8(1)(a).

<sup>603</sup> *ibid* Sutter, G. *E-mail monitoring and interception 2001* (2001) 3 Electronic Business Law 2, 3.

web usage through obtaining traffic data<sup>604</sup> and requiring communication service providers to assist investigations.<sup>605</sup> Consequently, unlike the US, the UK had a broad piece of legislation which directly related to intercepting Internet communications, enabling law enforcement to intercept email communications and monitor web usage therefore assisting the investigation of a serious crime perpetrated over or helped by the Internet prior to 9/11. It is unclear, however, whether this assisted with the prevention of terrorist communications or financial transactions carried out over the Internet before 9/11 as UK law specifically prohibits the use of intercept evidence in open court.<sup>606</sup> Additionally, the introduction of the Terrorism Act 2000 specifically defined it is an offence under s15(1)(a) if a person “*invites another person to provide money or other property...*” which will be used for terrorist activities, and under s15(3)(a) and (b) for donations which the donor knows or suspects their donation will be used for the purposes of terrorism,<sup>607</sup> thereby catching donors to websites or emails asking for funds which would be used for terrorist purposes. However, it is ambiguous as to whether these measures were used to online solicitations of donations immediately prior to 9/11.

### 3.3.3.2. Legitimate sources

---

<sup>604</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 21 and s. 22; Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 80-81.

<sup>605</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 22(4) and (6).

<sup>606</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 17.

NB. 1314 warrants were placed before the Home Secretary in 2001, after RIPA was introduced; Investigatory Powers Tribunal *Interception of Communications Commissioner's Annual Report for 2001* HC 1243 (HMSO, 31 October 2002), 4, para. 16 <<http://www.ipt-uk.com/docs/inter-comm-report-2001.pdf>> accessed November 2016.

<sup>607</sup> Terrorism Act 2000 c.11.

In 2000, the UK introduced the Financial Services and Markets Act which required the regulator of banks and financial services, the Financial Services Authority (FSA), to have regard to the use of financial institutions in financial crime,<sup>608</sup> as well as rule making powers on money laundering.<sup>609</sup> However, the FSA tended to be “e-neutral” on the issue of regulating online banks, although it did start to outline the potential risks of using online banking and e-commerce as well as their links to financial crime.<sup>610</sup> Nevertheless, it was doubtful whether this was used successfully to investigate the use of online financial transactions for terrorist purposes.

### **3.3.3.3. Cybercrime**

As with the US, the UK focused its efforts on overtly criminal use of the Internet and misuse of computers before 9/11. However, rather than have a single legislative instrument designed to combat both cyber-fraud and misuse of computers like the US, the UK instead used an extended interpretation of its traditional laws, including the Forgery and Counterfeiting Act 1981 and the Theft Act 1968 to combat elements of cybercrime. However, there were no convictions for cybercrime under the Forgery and Counterfeiting Act 1981, and it was eventually found inappropriate to combat cybercrime<sup>611</sup> due to its narrow interpretation. For example, the cases of *Gold and*

---

<sup>608</sup> Financial Services and Markets Act 2000 c.8, s. 6.

<sup>609</sup> Financial Services and Markets Act 2000 c.8, s. 146.

NB. The Act did not come into force until 1 December 2001.

<sup>610</sup> Financial Services Authority *Carol Sergeant, Director of Banks and Building Societies, Financial Services Authority* (29 March 2000)

<<http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2000/sp46.shtml>> accessed November 2016; Financial Services Authority *The Money Laundering Theme: Tackling our new responsibilities* (July 2001) which mentions non face-to-face banking and identity checks in Annex B

<[http://www.fsa.gov.uk/pubs/other/money\\_laundering.pdf](http://www.fsa.gov.uk/pubs/other/money_laundering.pdf)> accessed November 2016.

<sup>611</sup> Rider, B. *Cyber-organised crime – the impact of information technology on organised crime* (2001) 8(4) *Journal of Financial Crime* 332, 343.

*Schifreen*<sup>612</sup> failed on the basis that the hackers' access of the computer system did not include areas which stored and recorded information<sup>613</sup> and that prosecutors had 'forced' the language of the Act to apply in this instance.<sup>614</sup> Furthermore, existing criminal law on fraud did not cover the intention to defraud a machine,<sup>615</sup> highlighting a major gap in the UK's fight against the growing issue of criminal acts conducted over the Internet.

Consequently, the UK introduced the Computer Misuse Act 1990 (CMA), which dealt with the specific misuse of computers. Primarily, the CMA criminalised hacking under s. 1 (unauthorised access of computers),<sup>616</sup> unauthorised access of computers with intent to commit or facilitate further offences<sup>617</sup> and unauthorised access with intent to impair, or recklessness as to impairing, the operation of a computer.<sup>618</sup> Furthermore, s. 4 of the Computer Misuse Act addresses the issue of jurisdiction, by extending the territorial scope to allow prosecution if there is a material link, regardless of whether the offender was actually in the country or not at the time of the offence.<sup>619</sup> As a result, the CMA allowed law enforcement authorities to prosecute specific computer-related offences,<sup>620</sup> wherever they were committed, thereby increasing the UK's ability to combat the misuse of computers.

---

<sup>612</sup> *R v Gold and Shifreen* (1987) 3 All ER 618; (1987) 3 WLR 803 (C/A); (1988) 2 All ER 186; [1988] A.C. 1063.

NB. This case was decided upon the basis that a computer was a genuine instrument and intangible, capable of being both the deceiver and the deceived.

<sup>613</sup> Law Commission *Criminal Law: Computer Misuse* Cm819 (HMSO, October 1989), 9, para. 2.3 <<http://www.bailii.org/ew/other/EWLC/1989/186.pdf>> accessed November 2016.

<sup>614</sup> Bell, R.E. *The prosecution of computer crime* (2002) 9(4) *Journal of Financial Crime* 308, 318.

<sup>615</sup> *ibid* Rider, B. *Cyber-organised crime – the impact of information technology on organised crime* (2001) 8(4) *Journal of Financial Crime* 332, 343; Law Commission Report 9, para. 2.4.

<sup>616</sup> Computer Misuse Act 1990 c.18, s. 1(1)-(3); *ibid* Bell, R.E., 309.

<sup>617</sup> Computer Misuse Act 1990 c.18, s. 2(1)-(5); *ibid* Rider, B., 343.

<sup>618</sup> Computer Misuse Act 1990 c.18, s. 3(1)-(6); *ibid* Rider, B., 343.

<sup>619</sup> *ibid* Rider, B., 343.

<sup>620</sup> Computer Misuse Act 1990 c.18, s. 1-3.

However, the CMA was devoted primarily to the computer crime of hacking and impairment of computers, or “unauthorised access”, leaving it up to courts and prosecutors to determine fraud and other elements of cybercrime through traditional statutes. Moreover, the CMA highlighted a number of problems, for instance regarding the decision of prosecutors to apply either the CMA or the Theft Act 1968 when taking computer-related fraud to court.<sup>621</sup> Furthermore, there were few convictions or prosecutions for the facilitation of other offences (e.g. fraud) under s. 2 of the CMA, with the Home Office in 2004 showing that between 1990 and 2001, 35 were brought to court, with 14 being found guilty,<sup>622</sup> compared with 116 cases brought and 54 convictions under s. 3 of the Act.<sup>623</sup> Moreover, the CMA exposed difficulties for the courts when interpreting the meaning of “unauthorised access” of a computer,<sup>624</sup> only settling the issue in 1999<sup>625</sup> and making prosecutors cautious of bringing CMA-related charges to court.<sup>626</sup> As a result, the CMA was under-used by law enforcement against cybercrime, showing gaps in the UK’s anti-cybercrime legislation before 9/11. Additionally, as with the US’s Computer Fraud and Abuse Act, the CMA only applies to

---

<sup>621</sup> *ibid* Bell, R.E., 318-320.

<sup>622</sup> Information compiled from Written Evidence by the Home Office (CMA Regional Statistics) for the All Party Parliamentary Internet Group’s *Inquiry on the Computer Misuse Act* (2004) <<http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/computer-misuse-inquiry-written-evidence.html>> accessed November 2016; this is in comparison with 54 convictions out of 116 in the same period under s. 3 CMA.

<sup>623</sup> *ibid*.

<sup>624</sup> *DPP v Bignall* [1998] 1 Cr. App. R. 1; (1997) 161 J.P. 541; [1997-98] Info. T.L.R. 168; [1998] I.T.C.L.R. 33; [1998] *Masons C.L.R. Rep.* 141; [1998] *Crim. L.R.* 53; (1997); CMA was interpreted narrowly on appeal, meaning that employees who misused information from company computers were exempt from prosecution.

<sup>625</sup> Bell, R.E. *The prosecution of computer crime* (2002) 9(4) *Journal of Financial Crime* 308, 319; *R v Bow Street Metropolitan Stipendiary Magistrate and Another, ex parte Government of the United States of America* [2000] 2 AC 216 [1999] 3 W.L.R. 620; [1999] 4 All E.R. 1; [2000] 1 Cr. App. R. 61.

<sup>626</sup> *ibid*.

overtly criminal use of computers, rather than legal use for an eventually illegal purpose. Therefore, the CMA showed its inability to keep pace with terrorists and their use of evolving technology.

Nevertheless, the Council of Europe, of which the UK is a member, was particularly active in the area of cybercrime, first adopting Recommendation (89) 9 in 1989 which recommended that Member States include guidelines<sup>627</sup> by the European Committee on Crime Problems on computer crime (i.e. protection of data integrity) in national criminal legislation.<sup>628</sup> Additionally, in 1995 the Council adopted Recommendation (95) 13, which pointed out “*the principles that should guide states and their investigating authorities in the field of information technology*”,<sup>629</sup> highlighting the need for international co-operation and guiding Member States towards using technical surveillance<sup>630</sup> and gathering electronic evidence.<sup>631</sup> Furthermore, the Council’s Committee on Crime in Cyber-Space submitted the Convention on Cybercrime 2001, which has become a potentially important instrument in the international<sup>632</sup> fight against cybercrime and terrorist use of the Internet. Primarily, this expanded the scope of cybercrime from specific offences against computers to include other types of cybercrime which were computer-related. For instance, under Title 2, it is requested that

---

<sup>627</sup> NB. These were voluntary, non-binding guidelines and were therefore soft law.

<sup>628</sup> Council of Europe Recommendation R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime, s. 1 <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f1094>> accessed April 2018.

<sup>629</sup> Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223, 168.

<sup>630</sup> *ibid* Brenner, S. & Goodman, M., 169; Council of Europe Recommendation (95) 13 Concerning problems of criminal procedural law connected with information technology (11 September 1995), s. 5-8 <[https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/as-set\\_publisher/aDXmrol0vvsU/content/recommendation-no-r-95-13-of-the-committee-of-ministers-to-member-states-concerning-problems-of-criminal-procedural-law-connected-with-information-tec?\\_101\\_INSTANCE\\_aDXmrol0vvsU\\_viewMode=view/&desktop=false](https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/as-set_publisher/aDXmrol0vvsU/content/recommendation-no-r-95-13-of-the-committee-of-ministers-to-member-states-concerning-problems-of-criminal-procedural-law-connected-with-information-tec?_101_INSTANCE_aDXmrol0vvsU_viewMode=view/&desktop=false)> accessed April 2018.

<sup>631</sup> *ibid* Brenner, S. & Goodman, M., 169; *ibid* Council of Europe Recommendation (95) 13, s. 13.

<sup>632</sup> NB. This is defined as international as non-Member States of the Council of Europe also signed the Convention including the United States, Canada, Japan and South Africa, European Treaty Series No. 185 Convention on Cybercrime (23 November 2001) <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>> accessed November 2016.

Member States specifically legislate against computer-related offences such as forgery and fraud.<sup>633</sup> Moreover, law enforcement authorities are aided in their investigations, through the preservation of stored computer data<sup>634</sup> and traffic data<sup>635</sup> and the ability to intercept content data.<sup>636</sup> Additionally, the issue of jurisdiction is addressed by s. 3 of the Convention, guiding Member States to adopt legislation to establish jurisdiction over an offence<sup>637</sup> and highlighting the need for international co-operation<sup>638</sup> through extradition<sup>639</sup> and MLA treaties.<sup>640</sup> Consequently, the Convention on Cybercrime represented the first international instrument which comprehensively dealt with the problems involved in investigating cybercrime. Nevertheless, the UK, although signing it in 2001, only ratified its terms in 2011.<sup>641</sup>

Therefore, prior to 9/11 and, despite making significant steps towards intercepting Internet communications, the UK's computer crime legislation had lack of focus on the specific ways that terrorists use the Internet, instead concentrating on the "unauthorised access" of a computer and data protection rather than the use of the Internet to legally solicit donations and legally channel terrorist finances. Indeed, it was not until 2006 that the Theft Act 1968 was updated to include fraud by electronic means.<sup>642</sup>

---

<sup>633</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), s. 1 Title 2, Articles 7 and 8 <<http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>> accessed November 2016.

<sup>634</sup> *ibid* s. 2 Title 1, Article 16.

<sup>635</sup> *ibid* Article 17(1)(a).

<sup>636</sup> *ibid* Title 5, Article 21.

<sup>637</sup> *ibid* s. 3, Article 22.

<sup>638</sup> *ibid* Chapter III, Title 1, Article 23.

<sup>639</sup> *ibid* Chapter III, Title 2, Article 24.

<sup>640</sup> *ibid* Chapter III, Title 3, Articles 25 and 26.

<sup>641</sup> The UK signed the Convention on 23 November 2001 and ratified its terms on 25 May 2011. The date for entry into force was on 1 September 2011 <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>> accessed November 2016.

<sup>642</sup> Fraud Act 2006 c.35, s. 6 creates a new offence of obtaining and possessing "articles" for use in fraud so as to include electronic programmes and new technologies for obtaining property by fraud (see also s. 8) and Schedule I s7(3) amending Theft Act 1968 c.60 s. 9 to include an account with an

### 3.3.4. Saudi Arabia

Prior to 9/11 and the Bali bombings, it was evident that, unlike the US and the UK, which focused on data protection rather than censorship, some Middle Eastern countries had measures which enabled surveillance of the Internet through Internet Service Providers, focusing on content-related computer offences such as pornography. Furthermore, Saudi Arabia has state-owned telecommunications companies which enables it to have some measure of control over content distributed by Internet Service Providers.<sup>643</sup> These potentially had the ability to combat some types of cybercrime, including propaganda and forms of “hate speech” from terrorist organisations.<sup>644</sup> However, it was equally clear that the focus of some countries was on censorship and control by Government against morality or opposition to policies rather than the prevention of cybercrime or terrorist financing over the Internet, highlighting a number of gaps within legislation.

---

issuer of electronic money, as defined in the Financial Services and Markets Act 2000 c.8; Ormerod, D. & Williams, D. *The Fraud Act* (Legislative Comment) (2007) 1 Archbold News 6-9, 8.

<sup>643</sup> In Saudi Arabia, the Saudi Telecom Company owns a monopoly over Internet access and provides permission for other ISPs to operate in the country. Although it officially became incorporated in 1998 and the Government of Saudi Arabia sold 30% of its shares in 2002; Saudi Telecom Company *Annual Report for STC 2009*, 50 <<https://www.stc.com.sa/wps/wcm/connect/english/stc/resources/9/6/964cbd96-c271-4dfe-9331-33b6d70d93a9/annual-report2009.pdf>> accessed April 2018; the Government still owns 70% of the company - Saudi Telecom Company *Consolidated Financial Statements for the Year Ended 31 December 2015*, 7 <<https://www.stc.com.sa/wps/wcm/connect/english/stc/resources/8/c/8ccc40b1-82c2-4463-ad4d-a3e1e29851ee/2015.pdf>> accessed June 2018.

<sup>644</sup> The definition of “terrorist organisations” varies between jurisdictions – therefore it is in the context of groups who fall within the Security Council Resolution 1566’s scope of ‘terrorism’, S/RES/1566 (2004) Creation of working group to consider measures against individuals, groups and entities other than Al-Qaida/Taliban, paragraph 3.

NB. There have been a number of concerns raised by human rights organisations about the tactics of some jurisdictions in using their counter-terrorism laws to detain critics of Governments or human rights activists. E.g. Saudi Arabia - in 1993, members of the Committee for the Defense of Legitimate Rights were arrested and detained without trial for their criticism of the Government. They were arrested on the basis of breaching Article 39 of the Basic Law. Although not specifically imprisoned on the basis of terrorism, the use of ‘security of the State and its public image’ in the Article denotes a similar offence; Human Rights Watch *Precarious Justice: Arbitrary Detention and Unfair Trials in the Deficient Criminal Justice System of Saudi Arabia* (2008), 19-20 <[http://www.hrw.org/sites/default/files/reports/saudijustice0308\\_1.pdf](http://www.hrw.org/sites/default/files/reports/saudijustice0308_1.pdf)> accessed November 2016.



### 3.3.4.1. Direct solicitation of donations

Although it had initially allowed widespread public access to the Internet in 1999,<sup>645</sup> Saudi Arabia soon had a tough censorship regime, introducing its Internet Rules in February 2001. These outlined what types of data Internet users were to refrain from accessing or publishing, including “[a]nything liable to promote or incite crime, or advocate violence against others in any shape or form”,<sup>646</sup> Furthermore, unlike the US and the UK before 9/11, the Saudi Internet Rules set out a comprehensive framework of surveillance and barring techniques, including an electronic register of service users kept by Internet Service Providers,<sup>647</sup> provision of copies of this to the authorities<sup>648</sup> and restriction of Internet use by the King Abdulaziz City Science and Technology Unit.<sup>649</sup> Consequently, Saudi Arabia had the ability to track some ways of using the Internet to channel terrorist finances, for example, the solicitation of donations via websites and emails. Nevertheless, over 95% of the websites blocked by the Saudi Internet Services Unit<sup>650</sup> are those with sexually explicit content,<sup>651</sup> with the re-

---

<sup>645</sup> Despite launching a Government link to the Internet in 1994; OpenNet Initiative *Study on Saudi Arabia* (6 August 2009) <<http://opennet.net/studies/saudi>> accessed November 2016; Seymour, G. & Press, L. *The Global Diffusion of the Internet Project: An Initial Inductive Study* (1998), 210-211 <<http://mosaic.unomaha.edu/GDI1998/7HSAUDI.PDF>> accessed November 2016.

<sup>646</sup> Saudi Internet Rules, Council of Ministers Resolution, 12 February 2001 s. 8: <<https://albab.com/saudi-internet-rules-2001>> accessed April 2018.

<sup>647</sup> *ibid* Saudi Internet Rules, 12 February 2001.

<sup>648</sup> *ibid*.

<sup>649</sup> *ibid*; King Abdulaziz City Science and Technology website Internet Services Unit set up in 1998: <<https://www.kacst.edu.sa/eng/ScientificServices/ISU/Pages/History.aspx>> accessed April 2018.

<sup>650</sup> King Abdulaziz City Science and Technology Internet Services Unit <<https://www.kacst.edu.sa/eng/ScientificServices/InformationServices/Pages/landing.aspx>> accessed April 2018.

<sup>651</sup> Saudi Arabia Communications and Information Technology Commission *Introduction to Content Filtering, Communication and Information Technology Commission* <<http://www.citc.gov.sa/en/Pages/default.aspx>> accessed April 2018.

maintaining 5% being blocked by individual Internet users or on application by the Minister for the Interior.<sup>652</sup> It is therefore apparent that Saudi Arabia did not often use its Internet filtration technology to find websites directly related to terrorist organisations or cybercriminals prior to 9/11.<sup>653</sup> As Saudi Arabia did not issue a specific piece of legislation about posting Internet content until its Anti-Cybercrime Law of 2007 and, due to lack of reporting on decisions by the courts, it is unclear what average punishment was given to those who breached public morality through websites and messages. The likelihood is that punishment would be discretionary to a trial judge, either as a *hudud* crime if the communication fell under one of the six crimes outlined by the Qur'an<sup>654</sup> or as a *ta'azir* crime if the communication was not covered by *hudud* or *qisas* crimes.<sup>655</sup> Therefore it is ambiguous as to how Saudi Arabia would have prosecuted terrorist communications and solicitation of donations over the Internet prior to 9/11.

---

<sup>652</sup> United Nations Economic and Social Commission for Western Asia E/ESCWA/ICTD/2007/8 *Models for Cyber legislation in ESCWA Member Countries* (27 June 2007), 18 <<https://www.unescwa.org/publications/models-cyber-legislation-escwa-member-countries>> accessed April 2018.

<sup>653</sup> NB. The use of this system has been criticised as to its compatibility with human rights, which is essential for counter-terrorism measures; Chapter six, 6.2; Amnesty International cites the case of Fouad Ahmad al-Farhan, an Internet blogger detained without trial between 2007 and 2009 due to his criticisms of the Government of Saudi Arabia Amnesty International *Saudi Arabia* <<https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/>> accessed April 2018; also international criticism about the detention of Law Professor Mohammed Abdallah Al-Abdulkarim, who was detained in December 2010 after writing an online article alleging disagreements within the Saudi Royal Family; Usher, S. (BBC News, 7 December 2010) *Saudi royal succession: Professor detained over article* <<http://www.bbc.co.uk/news/world-middle-east-11936421>> accessed November 2016; Reporters sans Frontiers blacklisted Saudi Arabia due to its Internet censorship and detention of Government dissenters; Reporters without Borders *Saudi Arabia* <<https://rsf.org/en/saudi-arabia>> accessed April 2018; OpenNet Initiative also criticised Internet filtration of Saudi Arabia, OpenNet Initiative *Internet Filtering in Saudi Arabia* (2009) <[http://opennet.net/sites/opennet.net/files/ONI\\_SaudiArabia\\_2009.pdf](http://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf)> accessed November 2016.

<sup>654</sup> Apostasy, drinking wine, adultery, defamation, theft and highway robbery.

<sup>655</sup> Relating to the protection of the human life from all forms of physical violence.

### **3.3.4.2. Use of legitimate sources and 3. Cybercrime**<sup>656</sup>

Despite concerns about the appropriateness of the Saudi Government's stance on Internet censorship, the Saudi Arabian Monetary Agency highlighted growing concerns about the use of the Internet by cybercriminals and the vulnerability of Internet banking, issuing its Internet Banking Security Guidelines in May 2001.<sup>657</sup> The Guidelines identified problems with hacking<sup>658</sup> and "spoofing" (impersonating another computer or end user),<sup>659</sup> requesting that banks have authentication or "know your customer" procedures for Internet banking<sup>660</sup> and that secure web payments were introduced to prevent theft.<sup>661</sup> Consequently, it is apparent that Saudi Arabia was aware of the threat of cybercrime prior to 9/11, as well as the need for counteracting this through customer identification. Furthermore, Saudi Arabia had the capability of combating the problems cybercrime and abuse of online financial institutions created, although the Saudi Arabian Monetary Authority's Guidelines were "soft law" and not enshrined by legislation.

### **3.4. Conclusion**

Before 9/11, co-ordinated international action against both the financial crimes of money laundering and terrorist financing was lacking. With regard to money laundering, the UN's Vienna Convention was narrowly construed, limiting itself to money

---

<sup>656</sup> NB. Cybercrime and legitimate institutions are combined in this section as, prior to 9/11 there is little legislative or administrative action by all three countries on the issues of both legitimate online banking systems and cybercrime prior to 9/11.

<sup>657</sup> SAMA *Internet Banking Security Guidelines* <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?Paged=TRUE&p\\_SortBehavior=0&p\\_SAMAFilePublishDate=20100504+21:00:00&p\\_ID=10&PageFirstRow=16&&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?Paged=TRUE&p_SortBehavior=0&p_SAMAFilePublishDate=20100504+21:00:00&p_ID=10&PageFirstRow=16&&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed April 2018; replaced by the e-Banking Rules 2010 <[www.sama.gov.sa/en-US/Laws/BankingRules/E\\_banking\\_Rules.docx](http://www.sama.gov.sa/en-US/Laws/BankingRules/E_banking_Rules.docx)> accessed April 2018.

<sup>658</sup> *ibid* SAMA Internet Banking Security Guidelines, 2.2.

<sup>659</sup> *ibid* SAMA Internet Banking Security Guidelines, 2.2.

<sup>660</sup> *ibid* 3.3.

<sup>661</sup> *ibid*; Chapter four, 4.3.2.

laundering connected with drugs trafficking. Without a broader definition of money laundering, it was left up to individual Member States to either widen the scope of the Convention's application by applying it to other types of organised crime using money laundering, such as terrorism, or to adhere strictly to the Convention and only apply AML legislation to drugs trafficking-related offences. While some countries, such as the UK, had robust AML and CTF legislation, others, including the US, focused on AML laws or, like Saudi Arabia, had little to counter the flow of illicit finances. Therefore, this inconsistency in international regulation led to many variations within the investigation of money laundering and counter terrorist financing. Moreover, although international organisations, such as the FATF, Basel Committee and Egmont Group, widened the scope of AML provisions to other types of crime outside drugs trafficking, these measures were based on "soft" law, which is not binding on member countries.<sup>662</sup> Furthermore, though the UN had made a significant step against terrorist financing through its 1999 Convention, surprisingly few Member States, including the US, had signed up to or ratified its provisions before 9/11. Therefore, the majority of countries did not have the sufficient legal tools to investigate, track or prevent the flow of terrorist finances which were used in the events of 9/11.

In conjunction with these difficulties, it was not until after 9/11 and the Bali bombings in 2002 that the technological advancement of terrorists and their financing came to the attention of international and domestic authorities. Prior to 9/11, it was

---

<sup>662</sup> NB. International law overall recognises that state sovereignty means there is no formal obligation on territories to carry out international agreements unless by consent; Brand, R. *External Sovereignty and International Law* (1994) 18 Fordham Journal of International Law 1685, 1685; UN Charter 1945 at Article 2(1) and in Article 2(7), states that it could not "*intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter*" – the International Court of Justice confirmed this in 1949, stating "*between independent States, respect for territorial sovereignty is an essential foundation of international relations.*"; International Court of Justice Reports 1949, 4. However, non-intervention is on the proviso that Chapter VII of the Charter is not breached (i.e. international peace and security is not compromised).

apparent that international focus on Internet regulation was disparate and it was often left up to individual countries to decide on which areas of criminal activity over the Internet they would combat. The UN, by being reticent about Internet regulation and cybercrime, did not provide an international framework on which crimes should be focused on, along with what level of surveillance countries should use when investigating such activities. While organisations such as the OECD and G8 asked Member States to update their legal tools to involve Internet related crime, their suggestions were again based on soft law and did not require countries to implement them. Consequently, without such an international legislative framework, countries like the US and the UK concentrated upon overtly criminal acts perpetrated over the Internet, for instance, hacking, fraud, copyright and distribution of child pornography, while countries such as Saudi Arabia focused on website censorship and public morality. Without a cohesive international focus on the ways in which criminals use the Internet legally to further their aims, terrorist organisations' communications, legal solicitation of donations through charitable organisations and channelling funds through financial institutions would have slipped undetected past law enforcement authorities prior to 9/11. Furthermore, this disparity was reflected within Member States' attitudes towards data protection and surveillance of Internet communications, with the US having little legislative framework to deal with legal surveillance, the UK having comprehensive surveillance techniques and the Middle East having tough website filtration procedures and invasive surveillance on Internet communications. This would have created difficulties with MLA treaties, with some countries being unable to accept or provide evidence on the basis of data protection, causing investigations to falter. Consequently, there was little international balance between overly intrusive sur-

veillance and data protection before 9/11, generating problems when investigating cybercrime and legal use of the Internet for a criminal purpose. Against this background, the international community and law enforcement therefore faced an immense task of investigating and prosecuting terrorist uses of the Internet after the events of 9/11.

## **Chapter Four: The United States**

*“We will starve terrorists of funding, turn them one against another, drive them from place to place until there is no refuge or no rest...”*  
(President George W. Bush, 20 September 2001)<sup>663</sup>

### **4.1. Introduction**

As mentioned in chapter three, the United States (US) had focused its efforts primarily against money laundering prior to September 11, 2001 (9/11).<sup>664</sup> However, after 9/11, the US reaction against the specific offence of terrorist financing was rapid. Only 12 days after the attacks on the World Trade Centre in New York, and the Pentagon in Washington DC,<sup>665</sup> President Bush enacted Presidential Order 13,224,<sup>666</sup> finding that *“because of the pervasiveness and expansiveness of the financial foundation of foreign terrorists, financial sanctions may be appropriate for those foreign persons that support or otherwise associate with these foreign terrorists”*.<sup>667</sup> Consequently, it was

---

<sup>663</sup> President George W. Bush *Joint Session of Congress Concerning the September 11, 2001 Terrorist Attacks on America* Congressional Record Volume 147, S9553-S9555 (GPO, 20 September 2001) <<http://www.gpo.gov/fdsys/pkg/CREC-2001-09-20/pdf/CREC-2001-09-20-pt1-PgS9553-4.pdf#page=1>> accessed November 2016.

<sup>664</sup> Chapter three, 3.2.2. and 3.2.3.

<sup>665</sup> NB. Flight 93, which was meant to crash in Washington DC, was brought down near Shanksville, Pennsylvania before it could hit its designated target; *9/11 Commission Report* (22 July 2004), 10-14 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>666</sup> 23 September 2001, Executive powers granted under the International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35) (IEEPA), the National Emergencies Act of 1976 (Pub.L. 94–412, 90 Stat. 1255) (50 U.S.C. 1601 et seq.), §5 of the United Nations Participation Act of 1945 (Pub. L. 79-264, 59 Stat. 619) (22 U.S.C. 287c et seq.), as amended (22 U.S.C. 287c) (UNPA), and §301 of Title 3, United States Code.

<sup>667</sup> Executive Order 13,224 *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit, or Support Terrorism*.

deemed necessary to order the immediate blocking of assets associated with designated terrorist organisations<sup>668</sup> and individual donors,<sup>669</sup> as well as prohibit transactions with such organisations or individuals.<sup>670</sup> Furthermore, on 26 October 2001, less than six weeks after 9/11, the US took swift legislative steps to prevent and counteract the financing of terrorism.<sup>671</sup> The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ('USA PATRIOT Act') was passed by the US Senate,<sup>672</sup> providing new powers to disrupt and monitor terrorist financing, as well as introducing broad surveillance powers for law enforcement authorities to use when monitoring Internet communications. In particular, electronic surveillance<sup>673</sup> and roving wiretap clauses were accepted, unamended

---

<sup>668</sup> The US Secretary of State designates Foreign Terrorist Organisations in accordance with §219 of the Immigration and Nationality Act of 1952 (Pub.L. 82-414, 66 Stat. 163), 8 U.S.C. Ch. 12, §1189 which states under subsection (a):

(a) *Designation*

(1) *In general*

*The Secretary is authorized to designate an organization as a foreign terrorist organization in accordance with this subsection if the Secretary finds that—*

*(A) the organization is a foreign organization;*

*(B) the organization engages in terrorist activity (as defined in section 1182(a)(3)(B) of this title or terrorism (as defined in section 2656f(d)(2) of title 22), or retains the capability and intent to engage in terrorist activity or terrorism) <sup>11</sup>; and*

*(C) the terrorist activity or terrorism of the organization threatens the security of United States nationals or the national security of the United States.*

<sup>669</sup> Executive Order 13,224, s. 1.

<sup>670</sup> *ibid* s. 2.

<sup>671</sup> This met two of the aims as highlighted in Chapter one, 1.4.1.2.; Aim 1 - that of condemning terrorism as criminal and Aim 2 - taking steps to prevent and counteract through domestic measures, financing of terrorists and terrorist organisations under General Assembly Resolutions A/RES/49/60 Measures to eliminate international terrorism (9 December 1994) and A/RES/51/210 Measures to eliminate international terrorism (17 December 1996) - both were alluded to within the International Convention for the Suppression of the Financing of Terrorism 1999.

<sup>672</sup> Passed by House of Congress by 357 to 66 votes (25 October 2001) and passed by the Senate by 98 to 1; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137, 139; although [www.govtrack.us](http://www.govtrack.us) explains in more detail that the votes were as follows – in the House it was passed by 357 Yeas to 66 Nays with 9 not voting/not present and passed by the Senate by 98 Yeas to 1 Nay with 1 not voting/not present: <<http://www.govtrack.us/congress/bill.xpd?bill=h107-3162>> accessed November 2016; Gouvin, E.J. *Bringing out the big guns: The USA PATRIOT Act, Money Laundering and the war on Terrorism* (2003) 55 Baylor Law Review 956, 961.

<sup>673</sup> E.g. Pen registers and trap and trace amendments to the Foreign Intelligence Surveillance Act of 1978, under §214 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272), enabling the FBI to intercept electronic communications under its DCS1000 program (formerly known as Carnivore).



and with little debate,<sup>674</sup> despite previous criticisms by Congress about their compatibility with civil liberties and the Constitution.<sup>675</sup> This was perhaps, in part, due to tensions of an anthrax attack on Congress shortly before the Bill was passed,<sup>676</sup> as well as pressure to pass the legislation quickly by the then Attorney General, John Ashcroft.<sup>677</sup>

---

<sup>674</sup> Lodgson, K.R. *Who Knows you are Reading This? United States' Domestic Electronic Surveillance in a Post-9/11 World* (2008) *Journal of Law, Technology and Policy* 409, 419 whereby he states that not a single representative had time to read the Act properly before voting.

<sup>675</sup> Ludwig, T.P. *The Erosion of Online Privacy Rights in the recent tide of Terrorism* (2004) *Computer Law Review & Technology Journal* 131, 159; ; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 *European Journal of Law Reform* 137, 139; Feingold, R. (Sen.) *Congressional Record* (Government Publishing Office, Volume 147, Issue 144 S11020-S11023, 25 October 2001) <<http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi>> accessed November 2016 (NB. He was the only Senator to vote against the USA PATRIOT Act in the Senate); especially Feingold's comments about broad electronic surveillance measures, S11021-S11022; American Civil Liberties Union *Open letter to Senators* which explains that the Act was not subject to the Judiciary Committee's scrutiny, American Civil Liberties Union *Open letter to Senators* (2001) <<http://www.aclu.org/national-security/letter-senate-urging-rejection-final-version-usa-patriot-act>> accessed November 2016; American Civil Liberties Union ACLU "Bitterly Disappointed" in House-Senate Joint Passage of Anti-Terrorism Legislation (12 October 2001) <<http://www.aclu.org/national-security/aclu-bitterly-disappointed-house-senate-joint-passage-anti-terrorism-legislation>> accessed November 2016.

<sup>676</sup> Anthrax attacks occurred in October 2001 whereby a number of people, including two U.S. Senators, Tom Daschle (Senate Majority Leader) and Patrick Leahy (Senate Judiciary Committee Chairman), were sent anthrax through the post, just before the USA PATRIOT Act was passed; Harden, T. (The Telegraph, 18 October 2001) *Anthrax attack hits Congress* <<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1359800/Anthrax-attack-hits-Congress.html>> accessed November 2016; Lodgson, K.R. *Who Knows you are Reading This? United States' Domestic Electronic Surveillance in a Post-9/11 World* (2008) *Journal of Law, Technology and Policy* 409, 419.

<sup>677</sup> Attorney General Ashcroft wanted the USA PATRIOT Act to be passed within 'days' not weeks. McCarthy, M. *USA PATRIOT Act* (2002) 39 *Harvard Journal on Legislation* 435, 435-436; Attorney General Ashcroft's testimony before the Senate Committee on the Judiciary "The American people do not have the luxury of unlimited time in erecting the necessary defenses to future terrorist acts. The danger that darkened the United States of America and the civilized world on September 11 did not pass with the atrocities committed that day. Terrorism is a clear and present danger to Americans today" Attorney General John Ashcroft *Testimony before the Senate Committee on the Judiciary* (Department of Justice, 25 September 2001) <<http://www.justice.gov/archive/ag/testimony/2001/0925AttorneyGeneralJohnAshcroftTestimonybeforetheSenateCommitteeontheJudiciary.htm>> accessed November 2016; Attorney General Ashcroft, *Justice Department Briefing* (8 October 2001) <[https://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10\\_08.htm](https://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_08.htm)> accessed June 2018: "I also encourage the Congress to pass quickly the anti-terrorism legislation proposed by the administration so that law enforcement may have at its immediate disposal all appropriate anti-terrorism tools to fight this war."; Washington Post (8 October 2001) *Text: Attorney General John Ashcroft* <[http://www.washingtonpost.com/wp-srv/nation/attacked/transcripts/ashcroft\\_100801.htm](http://www.washingtonpost.com/wp-srv/nation/attacked/transcripts/ashcroft_100801.htm)> accessed November 2016.

NB. These views are perhaps a contrast to the way commentators, such as Chris Montgomery, feel years after 9/11. Montgomery, in particular, states that terrorism is "largely contained". Montgomery, C. *Can Brandenburg v Ohio survive the Internet and the Age of Terrorism? The Secret Weakening of a Venerable Doctrine* (2009) 70 *Ohio St. L.J.* 141, 141.

This chapter will assess counter-terrorist financing (CTF) provisions under Title III of the USA PATRIOT Act, as well as electronic surveillance provisions under Title II and their application to terrorist finances generated and channeled through the Internet. By studying legislative provisions under the three main ways of using the Internet to facilitate the financing of terrorism, firstly the effectiveness of these provisions, including whether they have been successful in catching terrorist financiers who conduct their business over the Internet, are assessed. The benchmark for effectiveness will be an assessment of how many cases have been taken to court, how many have been successfully prosecuted and how many acts have been prevented by US measures. For instance, the chapter will utilise judicial precedent as examples of US CTF measures, and assess whether US-based financial institutions and Internet Service Providers (ISPs) are capable of applying them for Internet payments and communications.

Secondly, the chapter examines their appropriateness, including whether the surveillance measures granted to law enforcement authorities under Title II have had an adverse impact on the majority of innocent US Internet users. In order to undertake this assessment, the chapter focuses on provisions of the Foreign Intelligence Surveillance Acts of 1978 and 2008 (FISA), as well as the Federal Bureau of Investigation's (FBI) actions on the issue, including the use of surveillance measures in Project Carnivore and its access to financial information stored on the European SWIFT banking database. SWIFT, in particular, will be used as an example of where the US had risked

its international co-operation obligations under Paragraph 3 of Security Council Resolution 1373.<sup>678</sup> Moreover, the chapter examines the actions and reactions of US Government departments, including the US Department of the Treasury and Department of Justice, agencies such as the Financial Crimes Enforcement Network (FinCEN), law enforcement authorities such as the FBI, as well as court decisions, to gauge whether the provisions enacted after 9/11 have been both appropriate and effective towards combating terrorist financing generated over the Internet. Finally, the chapter aims to make suggestions on improvements the US can make to its counter-terrorism legislation, in particular, on restoring the delicate balance between civil liberties and the need for surveillance measures as established in the seminal case of *Katz*.<sup>679</sup>

#### **4.2. Direct solicitation of donations**

Immediately after 9/11, it was apparent to law enforcement authorities that the terrorists who had carried out the attacks had used email and Internet communications to co-ordinate their actions.<sup>680</sup> Consequently, it was of paramount importance for US authorities to monitor email communications and to intercept suspected websites so

---

<sup>678</sup> UN Security Council Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts, para. 3(c) calls upon states to: *Cooperate, particularly through bilateral and multilateral arrangements and agreements, to prevent and suppress terrorist attacks and take action against perpetrators of such acts.*

<sup>679</sup> *United States v. Katz* 389 U.S. 347 (1967); a similar case which predates *Katz* and also dealt with warrantless electronic eavesdropping is *Berger v. New York* 388 U.S. 41 (1967) whereby the US Supreme Court held that a warrant allowing the ‘bugging’ of an attorney’s office without identifying a specific crime was contrary to the Fourth Amendment.

<sup>680</sup> E.g. Mohammed Atta sent an email to the other 9/11 terrorists stating: “*The semester begins in three more weeks. We’ve obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.*” [references to the buildings attacked] <<http://www.usip.org/files/resources/sr116.pdf>> accessed November 2016; Weimann, G. *www.terror.net – How Modern Terrorism Uses the Internet* (March 2004) Special Report 116 United States Institute of Peace 10; Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 138.

that both the planning of future terrorist acts, as well as their financing, could be prevented.<sup>681</sup> Therefore, surveillance measures were introduced under Title II of the USA PATRIOT Act.

#### **4.2.1. Websites**

The USA PATRIOT Act of 2001 has a number of provisions catching websites which openly solicit donations to designated terrorist organisations, increasing the effectiveness of such provisions. For instance, §225 of the Act provides an exemption of criminal or civil liability to ISPs who furnish “*any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance...*”.<sup>682</sup> According to Davis, this provision has the ability to allow ISPs to assist with law enforcement authorities when blocking websites which directly solicit donations without civil or criminal liability.<sup>683</sup> The Homeland Security Act of 2002 enables Government agencies to place pressure on ISPs,<sup>684</sup> by including ‘statutory authorisation’ with court-approved warrants and subpoenas within liability exemptions.<sup>685</sup> Nevertheless, the effectiveness of these provisions has been questioned by Davis, who explains that statutory measures only provide *encouragement* rather than a *mandatory* requirement

---

<sup>681</sup> Information posted on websites or even private chat rooms do not warrant Fourth Amendment protection as other users are not readily identifiable and they run the risk of undercover agents using the space: *United States v. Charbonneau* 979 F.Supp 1177 (S.D. Ohio 1997).

<sup>682</sup> §225 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272) amending §105 of the Foreign Intelligence Surveillance Act of 1978.

<sup>683</sup> Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 152.

<sup>684</sup> Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135) (6 U.S.C. Ch. 1, 101 et seq.); Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Az-zam.com* (2003) 1 JIJIS 88, 88.

<sup>685</sup> §225 Homeland Security Act of 2002 created the Cyber Security Enhancement Act of 2002 H.R. 3428 107<sup>th</sup> Congress; §225(h)(1) amends §2703(e) of Title 18 United States Code.

to report suspicious activity on the websites they host.<sup>686</sup> Consequently, this causes concern about the ability of federal agencies to keep track of extremist websites soliciting donations because ISPs do not necessarily have to report suspicious activities on the websites they host. By only providing an incentive through liability exemption, this does not properly ensure complete co-operation between federal agencies and ISPs when providing information about suspected websites. This is further highlighted by the reluctance of US courts to impose civil liability on ISPs unless it can be proved they “*were aware, or should have been aware...*”<sup>687</sup> that illegal activities were taking place on the websites they hosted.<sup>688</sup> This position is juxtaposed to mandatory reporting requirements for financial transactions over the Internet, which has increased co-operation and compliance in the banking system.<sup>689</sup> Instead, a mandatory requirement may heighten effectiveness and provide a proper public-private partnership when tracking extremist websites.

Additionally, the aversion of ISPs to shut down and monitor websites which directly solicit donations could be attributed to the sheer number of websites available globally. In March 2016, it was estimated that there were over 1 billion websites

---

<sup>686</sup> *ibid* Davis, B. R., 152; Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 11-15.

NB. In the US, the Protection of Children from Predators Act of 1998 (Pub. L. 105-314, 112 Stat 2974) (18 U.S.C. 1111 et seq.) §604 already outlines a mandatory requirement for Internet Service Providers to report ‘facts or circumstances’ relating to child pornography on the Internet to law enforcement authorities (§604(1)). Failure to do so results in a fine of at least \$50,000 (s. 604(3)).

<sup>687</sup> *ibid* Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 160.

<sup>688</sup> *E.g. Thomas Dart, Sheriff of Cook County v. Craigslist Inc.* 665 F. Supp. 2d 961 (N.D. Ill. Oct. 20, 2009), the United States District Court for the Northern District of Illinois held that the website Craigslist was civilly immune from the wrongs committed by its users (in this case, prostitution) through s. 230 (c)(1) and (2) of the Communications Decency Act of 1996 (Pub. L. 104-104, 110 Stat. 133) (47 U.S.C. 230); Ingber, A. *Cybercrime Control: Will Websites ever be accountable for the legal activities they profit from?* (2011-2012) 18 Cardozo Journal of Law and Gender 423, 424.

<sup>689</sup> Chapter three; chapter four, 4.4. for further information about mandatory reporting requirements under AML and CTF procedures.

registered on the Internet.<sup>690</sup> According to Davis and Lewis, the amount of extremist websites was also high by 2006,<sup>691</sup> a point confirmed by the Secretary General of INTERPOL, Ronald Noble, who explained in 2010 that the amount of extremist websites had ‘skyrocketed’ from 12 in 1998 to 4,500 in 2006.<sup>692</sup> Currently, there are very few complete statistics to suggest the total amount of extremist websites, but in the UK alone, more than 300,000 have been taken down by authorities in an 18 month period between 2014 and 2015.<sup>693</sup> Consequently, both law enforcement authorities and ISPs face a significant challenge in enforcing potential provisions and monitoring websites, as time and resources are often limited,<sup>694</sup> whilst jurisdictions and the ability to host websites are unlimited.

These points are compounded by the relative ease by which terrorist organisations and their online supporters can bypass national requirements. As evidenced by the case of *azzam.com*, a ‘pro-Jihad’ website which solicited donations for terrorist organisations, the flexibility of the Internet and the fact that ISPs can be located in different jurisdictions means that publishers are able to re-establish their websites and solicit donations elsewhere, causing complications when attempting to shut them

---

<sup>690</sup> Website figures are compiled from Netcraft, who explained that they had received responses to their March 2016 website survey from 1,003,887,790 websites; Netcraft *Web Server Survey* (March 2016) <<https://news.netcraft.com/archives/2016/03/18/march-2016-web-server-survey.html>> accessed March 2016.

<sup>691</sup> *ibid* Davis, B. R., 144; Lewis, J. A. *The Internet and Terrorism* (2005) 99 Am. Socy Intl. L Proc 112, 113.

<sup>692</sup> INTERPOL *Preventing Internet radicalization of youth requires global police network, INTERPOL Chief tells police summit - Secretary General warns of threat posed by 'skyrocketing' number of extremist websites* (21 September 2010) <<http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR072.asp>> accessed November 2016; BBC News (21 September 2010) *Extremist websites skyrocketing, says Interpol* <<http://www.bbc.co.uk/news/world-europe-11382124>> accessed November 2016; which also notes that the number could be much higher than the 4,500 estimated by Mr Noble.

<sup>693</sup> Mortimer, C. (The Independent, 17 December 2015) *More than 1,000 extremist websites taken down every week London Police Chief Sir Bernard Hogan-Howe says* <<http://www.independent.co.uk/news/uk/crime/more-than-1000-extremist-websites-taken-down-every-week-london-police-chief-sir-bernard-hogan-howe-a6776961.html>> accessed November 2016.

<sup>694</sup> *ibid* Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 155.

down or blocking access.<sup>695</sup> Bozonelos and Stocking further note in their analysis of the case that, since it was shut down in 2002, “*Azzam.com... has reappeared and disappeared again several times...*”-<sup>696</sup> a point chillingly highlighted by one of Azzam.com’s publishers, when he stated “*...One cannot shut down the Internet...*”.<sup>697</sup> Bypassing national legislation to continue an extremist website or to solicit donations can be as simple as changing a website’s name,<sup>698</sup> or changing ISPs to one which would host the content of their webpages<sup>699</sup>. Additionally, because the USA PATRIOT Act is limited by jurisdiction to US-based ISPs,<sup>700</sup> this exacerbates the problems law enforcement authorities encounter when shutting down or blocking websites which solicit donations for terrorist organisations, because there is neither an internationally agreed instrument on cybercrime,<sup>701</sup> nor an internationally agreed single definition of terrorism. Consequently, more multi-jurisdictional co-operation is needed

---

<sup>695</sup> *ibid* Davis, B. R., 141; The Babar Ahmad case has been ongoing for eight years; *United States v. Ahmad* 3:04CR301(MRK); *Ahmad v. United States* [2006] EWHC 2927 (Admin), [2007] H.R.L.R. 8 30 November 2006; *Babar Ahmad and Others v The United Kingdom* (Application nos. 24027/07, 11949/08 and 36742/08) [2012] ECHR 609. The extradition was ruled ‘partly admissible’. On 10 April 2012, the European Court of Human Rights found in *Babar Ahmad and Others v The United Kingdom* (Application nos. 24027/07, 11949/08 and 36742/08) [2012] ECHR 609 that Ahmad and four other suspected terrorists could be tried in the US. Ahmad was extradited with four other suspects to the US after a failed High Court bid on 5 October 2012: CBS New York (6 October 2012) *Five Terrorism Suspects Appear In Federal Courts In Manhattan And New Haven* <<http://newyork.cbslocal.com/2012/10/06/five-terrorism-suspects-appear-in-federal-courts-in-manhattan-and-new-haven/>> accessed November 2016. However, in 2014, he was sentenced to 12 and a half years with time served, meaning that he returned to the UK in 2015 a free man. See Casciani, D. (BBC News, 19 July 2015) *Cyber-jihadist Babar Ahmad released* <<http://www.bbc.co.uk/news/uk-33585959>> accessed November 2016.

<sup>696</sup> Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com* (2003) 1 JIJIS 88, 88.

<sup>697</sup> *ibid* Bozonelos, D. & Stocking, G., 97; *ibid* Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 141.

<sup>698</sup> Lewis, J.A. *The Internet and Terrorism* 99 Am. Socy Intl. L Proc 112 (2005), 114.

<sup>699</sup> *ibid* Bozonelos, D. & Stocking, G., 95.

<sup>700</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 12; *ibid* Davis, B. R., 159.

<sup>701</sup> NB. Because there is no UN Convention, there is no requirement for mutual legal assistance on cybercrime internationally to potentially 192 countries – the only such instrument would be the Council of Europe’s Convention on Cybercrime, European Treaty Series No. 185 (23 November 2001) which the US has signed and ratified <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG>> accessed November 2016.

to increase the effectiveness of CTF provisions and donations made over the Internet,<sup>702</sup> as evidenced by one of the aims of the 1999 Convention.<sup>703</sup> However this, in itself, is problematic. As Hinnen explains, ISPs can be situated in countries which may be unable or unwilling to co-operate with US law enforcement agencies when reporting suspicious or illicit activities.<sup>704</sup> Therefore, without international co-operation, the effectiveness of the use of ISPs as cyber-watchdogs is compromised, and the aim of the 1999 Convention to intensify and accelerate exchange of information about terrorist funds is not reached.<sup>705</sup>

Nevertheless, the USA PATRIOT Act strengthens existing provisions for material support to terrorism under §805<sup>706</sup> which could catch websites by extending the application of criminal penalties to material support outside the US.<sup>707</sup> Furthermore, §2339A of Title 18, US Code, as amended by the PATRIOT Act, catches solicitation

---

<sup>702</sup> Whitton, M., *Progression and Technological Advancement of Terrorist Financing: Are Current Laws Adequate?*, 6.

<sup>703</sup> Chapter one, 1.4.2.1.

<sup>704</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 12; E.g. Sudan, Iran and Syria may be unwilling to co-operate in such matters as they are listed as state sponsors of terrorism by the US Department of State *State Sponsors of Terrorism* <<http://www.state.gov/j/ct/list/c14151.htm>> accessed November 2016; Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 139; On the issue of international co-operation with regard to counter-terrorist financing, Iran and the Democratic People's Republic of North Korea are not on any membership on Financial Action Task Force (FATF) organisations and are considered a substantial risk for money laundering and terrorist financing. Cuba has only recently asked to be on the FATF subsidiary in South America, the GAFISUD, therefore will be deficient in counter-terrorist financing/anti-money laundering measures at an international level. Furthermore, the FATF has designated the following countries as “*Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies*” - Democratic People's Republic of Korea (DPRK), Ethiopia, Iran, Iraq, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia, Vanuatu, Yemen; Financial Action Task Force *Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies* <<http://www.fatf-gafi.org/countries/#high-risk>> accessed April 2018.

<sup>705</sup> Chapter one, 1.4.2.1.

<sup>706</sup> Amending §2339A of Title 18, US Code on terrorism.

<sup>707</sup> §805(a) (1)(A) USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272) – “by striking ‘within the United States’”.



of donations over the Internet by expanding material support requirements to ‘*intangible*’ property.<sup>708</sup> Yet, the success of these provisions when applied to websites is somewhat mixed. Indeed, from US Department of Justice figures in 2010, out of 150 defendants charged with material support, approximately half were convicted<sup>709</sup> and this becomes more difficult when Internet postings are included. For example, in the case of *Al-Hussayen*,<sup>710</sup> it was alleged that Samir Al-Hussayen had used his operational control of a number of Islamic charitable websites, including [www.iananet.org](http://www.iananet.org),<sup>711</sup> to raise funds for ‘*violent jihad*’<sup>712</sup> on behalf of the US designated terrorist organisation HAMAS.<sup>713</sup> Furthermore, it was alleged that one of the websites Al-Hussayen maintained and administrated, [www.islamway.com](http://www.islamway.com), had various articles promoting jihad in Israel with links to a page entitled “What is your role?”, whereby participants were openly solicited for donations to HAMAS via another website, [www.palestine-info.org](http://www.palestine-info.org).<sup>714</sup> Nevertheless, despite these charges and a ‘wealth’ of FBI evidence against him, Al-Hussayen was acquitted on all three material support counts,<sup>715</sup> with the jury being unable to reach a verdict on eight other counts, causing

---

<sup>708</sup> §2339A, Chapter 113B, Title 18 U.S.C.

<sup>709</sup> Vicini, J. (Reuters, 21 June 2010) *The Supreme Court on Monday upheld a law that bars Americans from providing support to foreign terrorist groups, rejecting arguments that it violated constitutional rights of free speech and association* <<http://www.reuters.com/article/2010/06/21/us-usa-security-court-idUSTRE65K4B420100621>> accessed November 2016; US Department of Justice *Letter from Ronald Welch, Assistant Attorney General, to Sen. Patrick Leahy and Sen. Jeff Sessions* (26 March 2010) <<http://www.justice.gov/cjs/docs/terrorism-crimes-letter.pdf>> accessed November 2016.

<sup>710</sup> *United States v. Al-Hussayen* CR03-048-C-EJL (D. Idaho 4 March 2004).

<sup>711</sup> Al-Hussayen operated and administered the content of websites for Islamic charities Islamic Assembly of North America (IANA) and the Al-Haramain Islamic Foundation – both of which were alleged to have had links to Islamic extremists and al-Qaeda by Saudi Arabian authorities. More will be detailed later in this Chapter and the thesis about both.

<sup>712</sup> *ibid* [11], [13].

<sup>713</sup> NB. HAMAS is designated as a terrorist organisation by the US therefore will be referred to as such in this chapter; US Department of State Bureau of Counterterrorism *Foreign Terrorist Organizations* <<https://www.state.gov/j/ct/rls/other/des/123085.htm>> accessed April 2018.

<sup>714</sup> *ibid* *United States v Al-Hussayen* [17].

<sup>715</sup> Williams, A.F. *Prosecuting Website Development under the Material Support to Terrorism Statutes: Time to fix what’s broken* (2008) 11 Legislation and Public Policy 365, 372-373.

the presiding judge to call a mistrial.<sup>716</sup> As Williams surmises, this may have been because of uncertainty on the application of First Amendment right of freedom of speech to websites, as well as lack of ‘hard evidence’ of terrorist support,<sup>717</sup> making a prosecution under the material support statutes of great risk, “*especially when one considers that neither of the material support statutes contains the words ‘Internet,’ ‘websites,’ or even ‘computer’*”.<sup>718</sup> As Williams further states, the vague wording of §2339A and B is unable to cover material support via websites as it does not give notice of potential criminal liability of website creation and maintenance.<sup>719</sup> Consequently, the case of Al-Hussayen highlights the problems of proving material support via a website in a court of law and, again, one of the aims of the 1999 Convention, that of prosecuting and punishing perpetrators of terrorist funding is unable to be fully met.<sup>720</sup>

However, in the case of *Kassir*,<sup>721</sup> five years later, a New York District Court found Kassir guilty of providing material support to al-Qaeda and other terrorist groups through his websites,<sup>722</sup> showing that the ‘material support’ provisions could

---

<sup>716</sup> *ibid* 373; Al-Hussayen waived his rights to object to deportation in return for the US authorities not to press the outstanding counts against him. He is now living in Saudi Arabia.

<sup>717</sup> *ibid* Williams, A.F., 378: “... Although the jury was looking for “hard evidence” of Al-Hussayen’s support for terrorism—e.g., providing weapons to terrorists, hiding terrorists, or even driving them to a target—they were instead provided with vast amounts of evidence showing that Al-Hussayen had built Internet websites that the government claimed were aimed at recruiting, funding, and encouraging jihadists in their worldwide campaigns of violence. The evidence of Internet activity apparently was not the “hard evidence” that the jurors expected for the prosecution of an alleged terrorist.”

<sup>718</sup> *ibid* Williams, A.F., 378.

<sup>719</sup> *ibid* Williams, A.F., 380.

<sup>720</sup> Chapter one, 1.4.2.1.

<sup>721</sup> *United States v. Kassir* 04 Cr. 356 (JFK), 2009 WL 910767, at \*4 (S.D.N.Y. 2 April, 2009); Kassir also appealed to the United States Court of Appeals in *United States v. Mustafa (Kassir)* (2. Cir 2011). The Court upheld the District Court’s original verdict.

<sup>722</sup> NB. It is worth noting that Kassir’s ‘material support’ was through providing training manuals and propaganda on his websites therefore was overtly providing material support – see *United States v. Mustafa (Kassir)* (2. Cir 2011). However, the same arguments would apply when openly soliciting donations on websites.

be used against website operators.<sup>723</sup> Nevertheless, Williams still makes a good argument about creating a new Internet-related provision to address the opaque language of §2339A and B so that a uniform application of criminal prosecution to material support via websites can occur.<sup>724</sup> Such a proposal would doubtless increase the effectiveness of material support requirements against websites and prevent conflicting decisions from the courts, as evidenced by *Al-Hussayen* and ensure that the US is more effective in prosecuting perpetrators of terrorist financing.<sup>725</sup>

Nonetheless, this type of provision would have to be balanced with Constitutional rights in order to be appropriate within the US's domestic law setting. Critics of the USA PATRIOT Act and its application to websites often cite the First Amendment of the Constitution which protects freedom of speech.<sup>726</sup> Yet, freedom of speech is not a complete protection. In the case of *Schenck v United States*,<sup>727</sup> the Supreme Court ruled that First Amendment rights were not absolute when national security was taken into consideration and that “*security of the community was paramount to an individual's freedom of speech...*”.<sup>728</sup> This view was upheld by the Supreme Court in *Brandenburg v Ohio*,<sup>729</sup> whereby it held that inflammatory speech could not be punished by the Government unless imminent lawless action ensued.<sup>730</sup> Therefore, the

---

<sup>723</sup> NB. This was because Kassir's co-conspirator and a number of witnesses testified against him, thereby proving beyond a reasonable doubt that he knowingly participated in materially supporting terrorist organisations – see *United States v. Mustafa (Kassir)* (2. Cir 2011).

<sup>724</sup> Williams, A. F. *Prosecuting Website Development under the Material Support to terrorism statutes: Time to fix what's broken* (2007-8) 11 N.Y.U. J. Legis & Pub Pol'y 365, 383-385; 401-402.

<sup>725</sup> *ibid*; Chapter one, 1.4.2.1.

<sup>726</sup> E.g. This was used as a defence in *Al-Hussayen*; *United States v Al-Hussayen* CR03-048-C-EJL (D. Idaho 4 March 2004); also azzam.com publishers claimed their First Amendment rights were being ‘trampled’ upon; Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com* (2003) 1 JIJIS 88, 88.

<sup>727</sup> *Schenck v. United States* 249 U.S. 47 (1919).

<sup>728</sup> *ibid* Bozonelos, D. & Stocking, G., 91; Berman, B. *Combating Terrorist Uses of the Internet* (2005) 99 American Society of International Law Proceedings 103,106.

<sup>729</sup> *Brandenburg v. Ohio* (1969) 395 U.S. 444.

<sup>730</sup> *ibid*. The court held: “*Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action*”.

argument of civil liberty should be balanced against the requirement for national security, making such measures on website surveillance appropriate in cases where national security is threatened.

Furthermore, in *Reno v American Civil Liberties Union*,<sup>731</sup> “the Supreme Court extend[ed] the First Amendment right of freedom of speech to sponsors of web pages...”.<sup>732</sup> Although 9/11 increased the activities of the FBI and other agencies when monitoring and shutting down extremist websites,<sup>733</sup> *Reno* still applies. Therefore, it is clear that procedures used in carrying out these actions - for instance, assessing whether they are US-based ISPs and whether US citizens are using them - have regard to the First and Fourth Amendments to the Constitution.<sup>734</sup> Furthermore, when the Department for Homeland Security issued its *National Strategy to Secure Cyberspace* in 2003 it specifically outlined that “care must be taken to respect privacy interests and other civil liberties”,<sup>735</sup> a point again highlighted by the 2011 Cyberspace Policy Review.<sup>736</sup> Consequently, it is apparent that Government agencies should have regard to the appropriateness of their actions under First Amendment rights for US citizens when dealing with terrorist websites.

Nevertheless, a concerning development with regard to freedom of speech has occurred since the seminal judgement on material support in *Holder v Humanitarian*

---

<sup>731</sup> *Reno v. American Civil Liberties Union* 521 U.S. 844 (1997).

<sup>732</sup> Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com* (2003) 1 JIJIS 88, 89.

<sup>733</sup> E.g. Use of “honey pot” websites by CIA to lure potential terrorist sympathisers, as well as monitoring by FBI, Department of Defense and Department of Justice; Theohary, C.A. & Rollins, J. R41674 CRS Report to Congress – *Terrorist Use of the Internet: Information Operations in Cyberspace* (8 March 2011), 6-7: <<http://www.fas.org/sgp/crs/terror/R41674.pdf>> accessed November 2016.

<sup>734</sup> *ibid* CRS Report, 8.

<sup>735</sup> Department for Homeland Security *National Strategy to Secure Cyberspace*, 14-15 <<https://www.dhs.gov/national-strategy-secure-cyberspace>> accessed April 2018.

<sup>736</sup> “The United States should adopt an integrated approach to national interests across a range of substantive areas—including cybersecurity and the protection of free speech and other civil liberties—to develop consistent policies.” Whitehouse Archives *Cyberspace Policy Review* (June 2011), 20 <<https://obamawhitehouse.archives.gov/cyberreview/documents/>> accessed April 2018.

*Law Project*.<sup>737</sup> In *United States v Mehanna*,<sup>738</sup> one of the earliest applications of *Humanitarian Law Project*, the court was presented with evidence of Mehanna's 'material support' of al-Qaeda through his Internet activity of postings, chat and translations,<sup>739</sup> which, the prosecution alleged, was providing 'expert advice and assistance'.<sup>740</sup> As Brown notes, *Humanitarian Law Project* attempts to draw a line between protected and unprotected speech and this rests primarily upon the relationship between the defendant and a designated terrorist organisation – i.e. that the material support was co-ordinated with and under direction of such an organisation.<sup>741</sup> However, in *Mehanna*, Brown contends that the alleged connection was where the Government's case was weakest under the *Humanitarian Law Project* test.<sup>742</sup> In fact, it may appear that the government in *Mehanna* "push[ed] the doctrinal envelope as to when a material support case can be brought",<sup>743</sup> expanding the reach of the material support statute by accepting unilateral action as a relationship.<sup>744</sup> Furthermore, as Brown outlines, the *Humanitarian Law Project* judgement failed to clarify how much of a relationship is needed between a defendant and a designated terrorist organisation to constitute material support, causing difficulty with interpretation in lower courts.<sup>745</sup> Therefore, although *Brandenburg* sets a line between freedom of speech and national

---

<sup>737</sup> *Holder v. Humanitarian Law Project et al* 130 S. Ct. 2705 (2010); see chapter four, 4.3.1. for further information; it clarified material support aspects of the USA PATRIOT Act and their constitutionality with regard to, for example, the First Amendment on freedom of speech; Brown, G.D. *Notes on a Terrorism Trial: Preventative Prosecution, 'Material Support' and the Role of the Judge after United States v. Mehanna* (5 April 2013), Boston College Law School Studies Research Paper Series, Research Paper 294, 21-23.

<sup>738</sup> *United States v. Mehanna* No. 09-cr-10017-GAO (D. Mass. 2011).

<sup>739</sup> Brown, G.D. *Notes on a Terrorism Trial: Preventative Prosecution, 'Material Support' and the Role of the Judge after United States v. Mehanna* (5 April 2013) Boston College Law School Studies Research Paper Series, Research Paper 294, 12.

<sup>740</sup> *ibid* 15.

<sup>741</sup> *ibid* 16.

<sup>742</sup> *ibid* 17.

<sup>743</sup> *ibid* 20.

<sup>744</sup> *ibid* 23-25.

<sup>745</sup> *ibid* 23.

security, the judgement of *Humanitarian Law Project* and its interpretation have concerning implications for those who post their views on websites or host supportive websites without soliciting donations directly. Despite these concerns however, since the *Humanitarian Law Project* verdict, material support charges rose from being present in 11.6% of terrorism-related cases in 2007 to 87.5% in 2011.<sup>746</sup> Therefore, it seems apparent that there is more of a move towards preventing extremist messaging online. Yet, despite several attempts to introduce more controls over freedom of speech,<sup>747</sup> there is more of a focus by US authorities to prevent extremism through community partnerships -<sup>748</sup> which will be explained in further depth in chapter five.<sup>749</sup> Therefore, it is apparent that, while the justice system and the Government views extremism one way, the application by law enforcement during their investigations and charges, may be very different.

#### **4.2.2. Electronic Communications**

The most controversial and most widely criticised aspects of the USA PATRIOT Act are its surveillance measures under Title II. In the aftermath of 9/11, it was highlighted

---

<sup>746</sup> Center on Law and Security *Terrorism Trial Report Card September 11 2001- September 11 2011* (New York University School of Law, 2011) <<http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf>> accessed November 2016.

NB. The Trial Report Cards go no further than 2011.

<sup>747</sup> Countering Violent Extremism Act (H.R.2899 — 114th Congress (2015-2016)) amending the Homeland Security Act 2002 an Office for Countering Violent Extremism could have been set up.

<sup>748</sup> For example, the FBI has the ‘Don’t Be a Puppet’ campaign for teenagers, so that they critically analyse what has been posted online; FBI Countering Violent Extremism *FBI Launches New Awareness Program for Teens* (8 February 2016) <<https://www.fbi.gov/news/stories/countering-violent-extremism>> accessed November 2016; there is also an Office for Community Partnerships provides assistance and support among the following streams for communities: (a) Community Engagement to build awareness and promote dialogue; (b) Field Support Expansion and Training to support Department for Homeland Security field staff; (c) Grant support through the Federal Emergency Management Agency to issue a notice of funding opportunities (d) Philanthropic Engagement, to maximise support for local communities and (e) Tech Sector Engagement, ‘to identify and amplify credible voices online and promote counter narratives against violent extremist messaging’; Department for Homeland Security *Countering Violent Extremism* <<https://www.dhs.gov/countering-violent-extremism>> accessed November 2016.

<sup>749</sup> Chapter five, 5.3.2.

that information about the hijackers were available on a number of Government and private databases,<sup>750</sup> therefore electronic surveillance was placed at the top of the political agenda<sup>751</sup> with a resolution to “*institute a program to use technology to better protect the nation against future terrorism*”.<sup>752</sup> Indeed, even before the USA PATRIOT Act was agreed by Congress, the FBI used Project Carnivore (by then renamed to the less controversial DCS1000), its computer surveillance programme, within hours of 9/11<sup>753</sup> and compelled several US-based ISPs to provide their email records.<sup>754</sup>

With regard to its effectiveness, primarily §204 of the PATRIOT Act amends §2511(2)(f) of Title 18 of the United States Code, extending the definition of ‘electronic communications’ to include email correspondence when monitoring and intercepting communications to investigate criminal offences such as terrorism.<sup>755</sup> Therefore, this provision enables law enforcement authorities to extend their surveillance techniques to communications over the Internet. For instance, in the cases of *United States v Jamie Paulin Ramirez*<sup>756</sup> and *United States v Colleen LaRose*<sup>757</sup> electronic evidence, through email communications, was extensively used to show that both

---

<sup>750</sup> Blasburg, S. *Law and Technology of Security Measures in the Wake of Terrorism* (2002) 8 B. U. J Sci. & Tech L. 721, 721.

<sup>751</sup> *ibid* Blasburg, S. 721-722 referencing President George W. Bush’s formal recognition in Department for Homeland Security *Using 21<sup>st</sup> Century Technology to Defend the Homeland* (19-21 *Securing the Homeland Strengthening the Nation*) (2003) <[http://www.dhs.gov/xlibrary/assets/homeland\\_security\\_book.pdf](http://www.dhs.gov/xlibrary/assets/homeland_security_book.pdf)> accessed November 2016.

<sup>752</sup> *ibid* Blasburg, S. 721.

<sup>753</sup> Madrinan, P. *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act 2001* 64 University of Pittsburgh Law Review 783 (2003), 789; *ibid* Blasburg, S. *Law and Technology of Security Measures in the Wake of Terrorism* (2002) 8 B. U. J Sci. & Tech L. 721, 725.

<sup>754</sup> *ibid* Blasburg.

NB. DCS1000 has not been used since 2002; Conway, M. *Terrorist ‘Use’ of the Internet and Fighting Back* (2006) 19 Information and Security 9, 22 <[https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura\\_conway.pdf](https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf)> accessed June 2018.

<sup>755</sup> Title 18, US Code, Chapter 119 §2511.

<sup>756</sup> *United States v. Jamie Paulin Ramirez* Eastern District of Pennsylvania 8 March 2011.

<sup>757</sup> *United States v. Colleen LaRose* E.D. Pa 1 February 2011.

LaRose and Ramirez had conspired to provide material support to terrorists.<sup>758</sup> Indeed, both cases highlight the effectiveness and the need for electronic surveillance and evidence-gathering techniques when prosecuting attempts to provide material support as well as the prevention of terrorist acts.

Furthermore, §206 and §214-215 of the USA PATRIOT Act amend FISA which greatly expands the areas in which law enforcement authorities can use surveillance techniques on the electronic communications on ‘foreign targets’. In particular, §214 and §216 allowed law enforcement authorities to use updated ‘pen/trap’ surveillance techniques, which originally monitored telephone numbers,<sup>759</sup> on the ‘non-content’ of suspect emails – i.e. address information about the sender and recipients, as

---

<sup>758</sup> NB. Both pleaded guilty and were co-defendants. In *LaRose*, Colleen LaRose pleaded guilty to conspiracy to provide material support for terrorists. She first came to the attention of authorities by posting comments and videos on the website YouTube under the username “JihadJane”. In the indictment for her case, it was alleged that one of her co-conspirators had posted the following on a terrorist website: “*I write this message on behalf of a respected sister. . . . The sister has been in touch with a brother . . . [who] has appealed for urgent funds stating that his resources are limited. . . . [T]he sister has provided me proofs that have confirmed that the brother is . . . true . . . . I know the sister and by Allah, all money will be transferred to her. The sister will then transfer the money to the brother via a method that I will not disclose*”; *United States v. Colleen R. LaRose Indictment* Criminal No 10- (4 March 2010), [18], 5 <<http://jnsllp.com/wp-content/uploads/2010/03/indictment.pdf>> accessed November 2016; Joint indictment of LaRose and Ramirez [36], 9, LaRose in an electronic communication said “*i will tell whoever i ask about sending funds to there, that the reason i want to send money there is for a sister, in other words i will lie to the kafir [sic - non-believer] animals.*”; LaRose plea memorandum, 5, in which it states that the Government could prove beyond reasonable doubt that she had discussed efforts to fundraise through electronic communications; *United States v. Colleen R. LaRose Government’s Change of Plea Memorandum* Criminal No. 10-123-01 (28 January 2011) <<http://www.jnsllp.com/wp-content/uploads/2011/02/plea-memo-larose.pdf>> accessed November 2016; In *Ramirez*, Jamie Paulin Ramirez also pleaded guilty to conspiracy to provide material support to terrorism which the Government could prove beyond all reasonable doubt; *United States v. Jamie Paulin Ramirez Government’s Change of Plea Memorandum* Criminal No. 10-123-02 (4 March 2011), 3-4 <<http://jnsllp.com/wp-content/uploads/2011/03/plea-memo-paulin-ramirez.pdf>> accessed November 2016; in October 2011, another two were charged in connection with material support offences in connection with LaRose; BBC News (20 October 2011) *Two charged over ‘Jihad Jane’ terror plot* <<http://www.bbc.co.uk/news/world-us-canada-15396382>> accessed November 2016; May 2012, Mohammed Hassan Khalid also pleaded guilty to conspiracy to provide material support to terrorists in connection with the LaRose and Ramirez case; US Department of Justice *Maryland Man Pleads Guilty to Conspiracy to Provide Material Support to Terrorists* (4 May 2012) <<http://www.justice.gov/opa/pr/2012/May/12-nsd-579.html>> accessed November 2016.

<sup>759</sup> *ibid* Madrinan, P. G. *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act 2001* (2003) 64 University of Pittsburgh Law Review 783, 791-792 – Madrinan uses quotes from USC Title 18 to provide definitions of pen registers and trap and trace devices – pen registers defined as ‘*a device which records or decodes electronic or other impulses which identify the numbers dialled or otherwise transmitted on the telephone line to which*



well as the subject line of the email.<sup>760</sup> Additionally, they can also be used on third party emails<sup>761</sup> and such court orders for pen/trap surveillance are now subject to nationwide jurisdiction under §216 and §220,<sup>762</sup> enabling law enforcement authorities to track communications without jurisdictional limitation. As Haglund argues, the updating of existing legislation to include terms relating to Internet communications for pen/trap measures means that courts are less constrained by “*outdated statutes*”<sup>763</sup> and have more ability to convict online criminal activity which was previously not covered.<sup>764</sup> Consequently, there is more potential for an effective process to capture terrorist communications.

Moreover, the PATRIOT Act and FISA provide further powers to law enforcement authorities to track terrorist financing through the use of National Security Letters (NSLs) under §505.<sup>765</sup> NSLs provide law enforcement with the power to require personal information, such as financial transactions and email communications<sup>766</sup>

---

*such device is attached*’ (§3127, Title 18 USC) and trap and trace devices defined as ‘*a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted*’ (§3127(4) Title 18 USC); Berkowitz, R. *Packet-sniffers and privacy: Why the no-suspicion-needed standard in the USA PATRIOT Act is unconstitutional* (2002-2003) 7 Computer L Rev & Tech. J.1, 2.

<sup>760</sup> Dean, S. *Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law under the Patriot Act* (2002-2003) 5 Tulane Journal of Technology and Intellectual Property 97, 102; Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137, 144; Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371, 390.

NB. The appropriateness of this will be discussed later.

<sup>761</sup> *ibid*; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137, 143.

<sup>762</sup> Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371, 395.

<sup>763</sup> Haglund, R. *Applying Pen Register and Trap and Trace Devices: As technology changes, is Congress or the Supreme Court best suited to Protect Fourth Amendment expectations of privacy?* (2002-2003) 5 Vanderbilt Journal of Entertainment Law & Practice 138, 145.

<sup>764</sup> *ibid*.

<sup>765</sup> ; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137, 145.

<sup>766</sup> *ibid*; Nieland, A.E. *National Security Letters and the amended PATRIOT Act* (2007) 92 Cornell Law Review 1201, 1207-1209 – NSLs were originally meant to be a *request* for information; they were not mandatory (1208) until the introduction of the Electronic Communications Privacy Act 1986.

from financial institutions and ISPs without the need for judicial oversight.<sup>767</sup> The USA PATRIOT Act widens their scope to enable most levels of law enforcement to self-certify NSLs,<sup>768</sup> and increase the type of information they may be able to access, including the address and subject lines of emails, as well as any website the subject may have ever visited.<sup>769</sup> Consequently, the use of NSLs, without the need for a court order, is a useful tool for investigating terrorist financing, as information gathered can be shared between federal agencies,<sup>770</sup> enabling agencies to identify the extent of a subject's financial networks and circle of associates,<sup>771</sup> as well as identifying the names and locations of suspected extremists.<sup>772</sup> Indeed, the FBI in 2006 explained that NSLs were “*an essential and indispensable intelligence tool*”.<sup>773</sup>

However, the effectiveness of NSLs has been somewhat limited, as it was shown that only one out of 192,499 NSLs led to a conviction on terrorism between 2003 and 2006.<sup>774</sup> Furthermore, as the Department of Justice outlined, in 2007 the FBI had found a number of administrative errors in filing and reporting NSLs.<sup>775</sup> In 2008, Lodgson argued that “*even the FBI has been unable to find a clear example*

---

<sup>767</sup> §2709(a), Chapter 121 of Title 18, U.S.C. *ibid* Nieland, A.E., 1213, when he mentions that the original provisions of the ECPA 1986 made no mention of judicial review of NSLs issued. Congress and the FBI themselves regulate the use of information gathered in NSLs under §2709(e) Title 18, U.S.C.

<sup>768</sup> *ibid*; §2709(b) Title 18, U.S.C.

<sup>769</sup> *ibid* Nieland, A.E., 1214.

<sup>770</sup> US Department of Justice *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (Office of the Inspector General, March 2008), 114 <<http://www.justice.gov/oig/special/s0803b/final.pdf>> accessed November 2016.

<sup>771</sup> *ibid* 115.

<sup>772</sup> *ibid*.

<sup>773</sup> *ibid* 114.

<sup>774</sup> Electronic Frontier Foundation *Ten Years After the Patriot Act, a Look at Three of the Most Dangerous Provisions Affecting Ordinary Americans* (12 October 2011) <<https://www EFF.org/deeplinks/2011/10/ten-years-later-look-three-scariest-provisions-usa-patriot-act>> accessed November 2016; US Department of Justice *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (Office of the Inspector General, March 2008) <<http://www.justice.gov/oig/special/s0803b/final.pdf>> accessed November 2016.

<sup>775</sup> *ibid* *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, 81-83.

where their expansive use of NSLs has made Americans safer”.<sup>776</sup> Consequently, the use of NSLs may not be completely effective in combating CTF, being unable to fully achieve the 1999 Convention’s aim of prevent and counteract movements of funds in accordance with international and domestic law.<sup>777</sup>

Overall, the effectiveness of the PATRIOT Act’s provisions is compromised by the *anonymity* of the Internet,<sup>778</sup> allowing the user to access information and to communicate from a large choice of anonymous and publicly used sources, including Internet cafés and public libraries,<sup>779</sup> protecting the user’s identity. Moreover, as Hinnen explains, users can further mask their identity by providing ISPs with false information about their identity.<sup>780</sup> As Davis also identifies, a variety of encryption techniques can be used in order to protect the user’s identity, including codes and stenography to disguise the message,<sup>781</sup> e-mail ‘*dead drops*’ - allowing access to an e-mail account and unsent messages without interception -<sup>782</sup> and sending encrypted messages embedded within spam.<sup>783</sup> Consequently, law enforcement agencies are faced with the difficult task of assessing whether e-mails and Internet communications contain information within them which solicits material support for a terrorist organisation. Evidently, due to the encryption techniques terrorists use, the effectiveness of surveillance is also affected.

---

<sup>776</sup> Lodgson, K.R. *Who Knows you are Reading This? United States’ Domestic Electronic Surveillance in a Post-9/11 World* (2008) *Journal of Law, Technology and Policy* 409, 420.

<sup>777</sup> Chapter one, 1.4.2.1.

<sup>778</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5, 11; Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 *CommLaw Conspectus* 119, 130-131.

<sup>779</sup> *ibid*.

<sup>780</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5, 13.

<sup>781</sup> Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 *CommLaw Conspectus* 119, 137.

<sup>782</sup> Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 *CommLaw Conspectus* 119, 138-9.

<sup>783</sup> *ibid* 140.

With regard to its appropriateness, the USA PATRIOT Act and former President Bush's Terrorist Surveillance Programme have been heavily criticised domestically, particularly because of their negative impact on Fourth Amendment rights of privacy and the use of warrants to access private information of US citizens. As mentioned previously in chapter three, the cases of *Olmstead* and *Katz* had balanced national security with civil liberties with regard to wiretapping telephones by requiring court orders for surveillance measures, supported by the Electronic Communications Privacy Act 1986.<sup>784</sup> Furthermore, in the case of *United States v. U.S. District Court*,<sup>785</sup> the court held that using the reason of "national security" to wiretap individuals without a warrant in domestic cases was insufficient to circumvent the Fourth Amendment rights of American citizens.<sup>786</sup> However, post-9/11, the expansion of surveillance provisions posed a significant problem with particular regard to email communications. Unlike trap and trace devices and pen registers used on telephone calls, whereby the content of the call can be separated from the addressing information through just providing a list of telephone numbers,<sup>787</sup> emails are sent to federal agencies as a "package" of both content (the body of the email) and non-content (addressor and addressee information, as well as the subject line of an email).<sup>788</sup> As Lee outlined, the FBI receives the full email and then uses programmes to separate out the content

---

<sup>784</sup> Chapter three, 3.3.2.1.

<sup>785</sup> *United States v. U.S. District Court* 407 U.S. 297 (1972).

<sup>786</sup> Lodgson, K.R. *Who knows you are reading this? The United States' domestic electronic surveillance in a post-9/11 world* (2008) *Journal of Law Technology & Policy* 409, 429; Barnum, D.G. *Warrantless electronic surveillance in national security cases: Lessons from America* (2006) 5 *European Human Rights Law Review* 514, 525, which is why the Foreign Intelligence Surveillance Act of 1978 is meant to be used for foreign surveillance targets only (527-528).

<sup>787</sup> Berkowitz, R. *Packet-sniffers and privacy: Why the no-suspicion-needed standard in the USA PATRIOT Act is unconstitutional* (2002-2003) 7 *Computer L Rev & Tech. J.* 1, 9.

<sup>788</sup> Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 *Rutgers Computer & Technology Law Review* 371, 392; *ibid* Berkowitz, 10-11; Nabbali, T. & Perry, M. *Going for the throat: Carnivore in an ECHELON world – Part II* (2004) 20(2) *Computer Law & Security Report* 84, 84.

from the non-content, depending on the amount of information it is allowed to access.<sup>789</sup> However, it has been noted that the Government “*cannot be trusted*”<sup>790</sup> not to access the content of emails and that to rely “*entirely on the Government’s word that it will not access content is entirely unacceptable and inconsistent with the Fourth Amendment...*”.<sup>791</sup> Consequently, the expansion of wiretapping under the PATRIOT Act based on pen registers and trap and trace devices designed for telephone calls potentially breaches the Fourth Amendment, as well as human rights elements of Article 15 of the Convention on Cybercrime, to which the US is a party.<sup>792</sup>

With regard to stored communications information under §215, Vervaele states that during the investigation of terrorism and related offences (such as material support), subpoenas for stored information such as e-mails, do not have to adhere to the US legal tenet of probable cause,<sup>793</sup> meaning that law enforcement authorities can, in effect, access stored communications “*...without judicial authorisation...*”.<sup>794</sup> Under FISA 1978, Vervaele further outlines that the subpoena is always needed with judicial authorisation; however, the legal justification is *lowered* under §212<sup>795</sup> as it “*need only be shown that the information is relevant for the ongoing investigation*

---

<sup>789</sup> *ibid* Lee, L.T., 392-393; *ibid* Berkowitz, R. 11-12.

<sup>790</sup> *ibid* Lee, L.T., 393; Dean, S. *Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law under the Patriot Act* (2003) 5 Tul. J. Tech. & Intell. Prop. 97, 107.

<sup>791</sup> *ibid* Lee, L.T., 393.

<sup>792</sup> Chapter one, 1.4.2.2.

<sup>793</sup> Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137; Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375, 395-7; Johnson, H.A. *The USA PATRIOT Act and Civil Liberties: A Closer Look* (USCAW Strategy Research Project, 15 March 2006) <<http://www.dtic.mil/dtic/tr/fulltext/u2/a449681.pdf>> accessed June 2018.

<sup>794</sup> *ibid* ; Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137.

<sup>795</sup> §225 Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135) (6 U.S.C. Ch. 1, 101 et seq.); Smith, M. RL31408 CRS Report to Congress *Internet Privacy: Overview and Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session* (2006), 8 <<https://www.everycrsreport.com/reports/RL31408.html>> accessed June 2018.

(*relevance standard*)”.<sup>796</sup> Additionally, under §206, for “roving wiretaps” on multiple telephone lines of a subject, there is no judicial oversight, including requirements for law enforcement authorities to report to the court issuing the warrant.<sup>797</sup> As Ludwig outlines, this has created concern amongst privacy advocates, as there are doubts that the government could remain within its constitutionally-defined boundaries when given such expansive powers combined with insufficient judicial oversight.<sup>798</sup> Moreover, the protection of the original PATRIOT Act, allowing “sunset” provisions (i.e. provisions set to expire or terminated unless made permanent)<sup>799</sup> on the most controversial surveillance powers, including §206 and §215, were reauthorised in 2006,<sup>800</sup> 2010<sup>801</sup> and 2011.<sup>802</sup> Consequently, enabling law enforcement agencies access to private telecommunications without sufficient checks by the judiciary, or adhering to the standard set by the law, Title II of the PATRIOT Act creates considerable concern

---

<sup>796</sup> §215 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272); Vervaele, J.A.E. *The Anti-terrorist legislation in the US: Inter Arma Silent Leges* (2005) 13(2) *European Journal of Crime, Criminal Law and Criminal Justice* 201, 219; *ibid* Blasburg, S. *Law and Technology of Security Measures in the Wake of Terrorism* (2002) 8 B. U. J. Sci. & Tech L. 721, 725; Wyden, R. (Sen.) *Law and Policy Efforts to balance security, privacy and civil liberties in post 9/11 America* (2006) 17 *Stanford Law and Policy Review* 331, 334.

<sup>797</sup> *ibid* Ludwig, T. P. *The erosion of privacy rights in the recent tide of terrorism* (2003-2004) 8 *Computer Law Review & Technology Journal* 131, 167; although Ludwig doesn’t specifically list which organisations and activists he refers to, but organisations such as the American Civil Liberties Union and Electronic Privacy Information Center have consistently raised concerns about wiretapping and the USA PATRIOT Act since its introduction in 2001.

<sup>798</sup> *ibid*.

<sup>799</sup> §224 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272).

<sup>800</sup> *ibid* Wyden, R. (Sen.) *Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America* (2006) 17 *Stan. L. and Pol’y Rev* 331, 335; USA PATRIOT Act Improvement and Reauthorization Act of 2005 (Pub. L. 109-177, 120 Stat. 192).

NB. 14 out of 16 provisions set to expire in 2006 were made permanent – only “roving wiretaps” on multiple telephone lines under §206 and stored records access under §215 had further sunset provisions.

<sup>801</sup> H.R. 3961ENR (2010), Public Law No. 111-114, which extended provisions until 28 February 2011 <<http://www.gpo.gov/fdsys/pkg/PLAW-111publ141/html/PLAW-111publ141.htm>> accessed November 2016.

<sup>802</sup> The PATRIOT Sunsets Extension Act of 2011, (Pub. L. 112-114, 125 Stat. 216) (50 U.S.C. 1801) extended provisions until 1 June 2015; US Senate *PATRIOT Act Reauthorization s.1038 Legislative Bulletin* (Democratic Policy and Communications Center, 23 May 2011) <<http://dpc.senate.gov/docs/lb-112-1-14.pdf>> accessed November 2016.

about the forfeiture of civil liberties, as well as the ability of the Act to comply with the Convention on Cybercrime.<sup>803</sup>

Furthermore, Ludwig states that FISA is meant to be “*part of the dividing wall that Congress erected between domestic law enforcement and foreign intelligence agencies*”.<sup>804</sup> However, as Ludwig outlines, due to the enactment of the PATRIOT Act, many of these barriers have become blurred, potentially catching domestic communications and law enforcement investigations.<sup>805</sup> Donohue also explains that the PATRIOT Act *lowered* the bar for surveillance applications from foreign intelligence from being “the” sole reason for surveillance to being “a significant reason”<sup>806</sup>, meaning that the gap between the FBI’s prosecution and intelligence functions had been closed<sup>807</sup> and allowing FISA surveillance to be used in ordinary criminal cases rather than national security.<sup>808</sup> Therefore, changes to FISA have raised serious concerns about the applicability of emergency provisions to ordinary criminal activity.

Nevertheless, some concessions were made in the FISA Amendments Act 2008.<sup>809</sup> For example, the Foreign Intelligence Surveillance Court (FISC) now monitors warrantless surveillance -<sup>810</sup> although this had *already* been a requirement of

---

<sup>803</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Article 15; chapter one, 1.4.2.2.

<sup>804</sup> *ibid* Ludwig, T. P. *The erosion of privacy rights in the recent tide of terrorism* (2003-2004) 8 Computer Law Review & Technology Journal 131, 164.

<sup>805</sup> *ibid* Ludwig, T. P. *The erosion of privacy rights in the recent tide of terrorism* (2003-2004) 8 Computer Law Review & Technology Journal 131, 164-166; Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371, 387.

<sup>806</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 233.

<sup>807</sup> *ibid*. Donohue also notes that the FIS Court raised concerns about this tactic but the Government won on appeal, creating serious constitutional concerns.

<sup>808</sup> *ibid* 234.

<sup>809</sup> Foreign Intelligence Surveillance Act of 1978 Amendments Act 2008 (Pub. L. 110-261, 122 Stat. 2436) (50 U.S.C. Ch 36 1801 et seq.) <<https://www.gpo.gov/fdsys/pkg/PLAW-110publ261/pdf/PLAW-110publ261.pdf>> accessed April 2018.

<sup>810</sup> §109 FISA Amendment Act 2008; Eisler, P. (USA Today, 10 July 2008) *Senate OKs Surveillance Revamp* <[www.usatoday.com/printedition/news/20080710/a\\_fisa10.art.htm](http://www.usatoday.com/printedition/news/20080710/a_fisa10.art.htm)> accessed November 2016; US Department of Justice *Letter to Nancy Pelosi, Speaker at the House of Representatives from*

FISA 1978<sup>811</sup> potentially striking a balance between requirements of speed to intercept communications and constitutionality.<sup>812</sup> Furthermore, FISA 2008 requires six-monthly reports to be submitted to Congress of surveillance measures, providing some oversight of its measures.<sup>813</sup> Nevertheless, the Act was criticised by the American Civil Liberties Union (ACLU), who stated that it “...gives the government new spying powers including the power to conduct dragnet surveillance of Americans’ international communications...”<sup>814</sup> and pursued court action against the US Government - which failed in front of the Supreme Court in 2013.<sup>815</sup> Additionally, in 2011 and 2012, the FIS Court received a total of 3,465 applications for electronic surveillance by the US government, of which none were denied<sup>816</sup> and, between 2008 and 2012, out of 8,591 requests, only two were rejected, leading critics to describe the court as a “rubber-stamp” for the government’s surveillance programme.<sup>817</sup> Therefore, a number of concerns have been raised about the amount of applications approved, including the

---

*the Attorney General, Michael Mukasey and the Director of National Intelligence, J.M. McConnell* (19 June 2008), 1-2 <<http://www.justice.gov/archive/ll/docs/ag-dni-fisa-letter061908.pdf>> accessed November 2016.

<sup>811</sup> Under FISA 1978, Subchapter 1, §1803.

<sup>812</sup> *ibid* Mukasey and McConnell, 2.

<sup>813</sup> §1871(a) Chapter 35, U.S. Code 50; the Attorney General submits the reports.

<sup>814</sup> American Civil Liberties Union *ACLU sues over Unconstitutional Dragnet Wiretapping Law* (10 July 2008) <[www.aclu.org/safefree/nsaspying/35942prs20080710.html](http://www.aclu.org/safefree/nsaspying/35942prs20080710.html)> accessed November 2016.

<sup>815</sup> *Amnesty International USA et al. v. James R. Clapper Jr et al.* 638 F.3d 118 (2d Cir. 2011) which allowed the plaintiffs the right to challenge the constitutionality of wiretapping legislation; in September 2011, the United States Court of Appeals Second Circuit faced a split vote when discussing the Government’s appeal to have the case reheard in banc, leaving the prior judgment in force; on 26 February 2013, the Supreme Court held that the respondents’ challenge fell in *Clapper v. Amnesty International USA et al.* 638 F. 3d 118 <<http://www.law.cornell.edu/supremecourt/text/11-1025>> accessed November 2016.

<sup>816</sup> In 2011, 1,676 electronic surveillance applications were received and none were denied; US Department of Justice *FISA report 2011* (30 April 2012) <<http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>> accessed November 2016. In 2012, the court received 1,789 applications and none were denied; US Department of Justice *Letters from Peter J. Kadzik, Principal Deputy Assistant Attorney General, to Harry Reid, Majority Leader, US Senate, Nancy Pelosi, Minority Leader, US House of Representatives, Mitch McConnell, Minority Leader, US Senate, Eric Cantor, Majority Leader, US House of Representatives, John Boehner, Speaker, US House of Representatives, Joseph R. Biden Jr, President, US Senate, and Patrick J. Leahy, Chairman, Committee on the Judiciary* (30 April 2013), 1 <[http://www.justice.gov/nsd/foia/foia\\_library/2012fisa-ltr.pdf](http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf)> accessed November 2016.

<sup>817</sup> EPIC *Foreign Intelligence Surveillance Act Court Orders 1979-2012* <[http://epic.org/privacy/wiretap/stats/fisa\\_stats.html](http://epic.org/privacy/wiretap/stats/fisa_stats.html)> accessed November 2016.



lack of challenge available to the Court's decisions (as only one party, the US government, is present) as well as issues surrounding availability of court opinions to allow scrutiny.<sup>818</sup> In 2008, Yahoo! also fought a warrantless request to provide email communications before the FIS Court, which was subsequently refused.<sup>819</sup> Moreover, as the Internet is global, many electronic communications by US citizens will inevitably be caught by the FISA arrangements due to the fact that they can communicate with persons outside the US, thus affecting their rights under the Fourth Amendment.<sup>820</sup> Despite these concerns, including privacy amendments raised,<sup>821</sup> on 27<sup>th</sup> December 2012, Congress reauthorised FISA 2008 for a further five years.<sup>822</sup> However, the United States Congress passed the United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA Freedom" Act),<sup>823</sup> with new prohibitions on bulk collection of pen registers, as well as trap and trace devices under FISA<sup>824</sup> and NSLs.<sup>825</sup> Such a volte face by the US has shown that, despite the further encroachment of surveillance techniques on private citizens

---

<sup>818</sup> Barnes, R. (Washington Post, 7 June 2013) *Secrecy of surveillance programs blunt challenges about legality* <[http://articles.washingtonpost.com/2013-06-07/politics/39815715\\_1\\_warrantless-surveillance-government-surveillance-president-obama](http://articles.washingtonpost.com/2013-06-07/politics/39815715_1_warrantless-surveillance-government-surveillance-president-obama)> accessed November 2016; Congressional Record *Sen. Ron Wyden speech* (GPO S8389, 27 December 2012) <<http://www.gpo.gov/fdsys/pkg/CREC-2012-12-27/pdf/CREC-2012-12-27-pt1-PgS8384-2.pdf#page=4>> accessed November 2016.

NB. Sen. Wyden also mentioned in his speech that, in 2009, the Obama administration proposed to publish some of the FIS Court's decisions (albeit redacted) on 'significant interpretations of law' but that none have ever been released (ibid).

<sup>819</sup> Cain, C. (New York Times Daily Report, 14 June 2013) *Secret Court Ruling in 2008 Put Technology Companies in Bind* <<http://bits.blogs.nytimes.com/2013/06/14/daily-report-secret-court-ruling-in-2008-put-technology-companies-in-bind/?ref=foreignintelligencesurveillanceactfisa>> accessed November 2016.

<sup>820</sup> ibid *Sen. Ron Wyden speech* (27 December 2012).

<sup>821</sup> ibid *Sen. Ron Wyden speech*, S8384-S (27 December 2012), including concerns about the fact that the FIS Court does not approve individual applications, it just reviews the government's surveillance techniques on an annual basis as well as the fact that it conducts its reviews in secret (S8389).

<sup>822</sup> By 73 to 23 with 4 abstentions, *Roll Call Vote 112th Congress - 2nd Session* (28 December 2012) <[http://www.senate.gov/legislative/LIS/roll\\_call\\_lists/roll\\_call\\_vote\\_cfm.cfm?congress=112&session=2&vote=00236](http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=112&session=2&vote=00236)> accessed November 2016.

<sup>823</sup> Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA Freedom Act") (Pub. L. 114-23, 120 Stat 200) (50 U.S.C. 1801).

<sup>824</sup> §201 USA Freedom Act of 2015.

<sup>825</sup> ibid §501.

after 9/11, the US is now finding more of a balance with appropriately intercepting communications.

Concerns about a lack of balance when accessing content of electronic communications under FISA and the Amendment Act reached a pinnacle in June 2013, when a former National Security Agency (NSA) operative leaked details of their data collection programme PRISM.<sup>826</sup> Under PRISM, which has been in use since 2007,<sup>827</sup> and uses §702 of FISA as its basis, both the non-content and the content of communications can be accessed directly from ISP servers.<sup>828</sup> The US government has maintained that this programme is necessary due to national security, that it is constitutional as it does not access internal American communications directly,<sup>829</sup> is regularly reviewed by the FIS Court, the Executive and Congress,<sup>830</sup> and that it has prevented potential terrorist attacks such as the plot to blow up the New York Subway in 2009.<sup>831</sup>

---

<sup>826</sup> Edward Snowden, the NSA operative, has received asylum in Russia for the last three years, despite a formal extradition request from the US. President Obama, in his last few weeks in office, has refused to pardon him for his crimes as he has not yet appeared before a US Court to enter a plea; Blake, A. (The Washington Post, 18 November 2016) *Obama shrugs off Edward Snowden's plea for Presidential pardon* <<http://www.washingtontimes.com/news/2016/nov/18/obama-refuses-edward-snowdens-plea-presidential-pa/>> accessed November 2016.

<sup>827</sup> Protect America Act of 2007 (Pub.L. 110–55, 121 Stat. 552) (50 U.S.C. Ch. 36 1801 et seq.) enacted by S. 1927.

<sup>828</sup> Greenwald, G & MacAskill, E. (The Guardian, 7 June 2013) *NSA Prism program taps into user data of Apple, Google and others* <<http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>> accessed November 2016; Black, I. (The Guardian Newspaper, 10 June 2013) *NSA Spying Scandal: What we have learned* <<http://www.guardian.co.uk/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned>> accessed November 2016.

<sup>829</sup> Director of National Intelligence *Statement of the Director of National Intelligence, James R Clapper* (6 June 2013) <<https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>> accessed April 2018; Director of National Intelligence *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (8 June 2013) <[http://content.govdelivery.com/attachments/USODNI/2013/06/08/file\\_attachments/217069/Facts%2Bon%2Bthe%2BCollection%2Bof%2BIntelligence%2BPursuant%2Bto%2BSection%2B702.pdf](http://content.govdelivery.com/attachments/USODNI/2013/06/08/file_attachments/217069/Facts%2Bon%2Bthe%2BCollection%2Bof%2BIntelligence%2BPursuant%2Bto%2BSection%2B702.pdf)> accessed November 2016.

<sup>830</sup> *ibid.*

<sup>831</sup> Schmitt, E., Sanger, D.E. & Savage, S. (New York Times, 7 June 2013) *Administration says mining of data is crucial to fight terror* <<http://www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?hpw>> accessed November 2016; Lister, T. & Cruickshank, P. (CNN, 11 June 2013) *Intercepted communications called critical in terror investigations* <<http://edition.cnn.com/2013/06/11/us/nsa-data-gathering-impact>> accessed November 2016; BBC News (13 June 2013) *NSA Chief says data disrupted 'dozens' of plots* <<http://www.bbc.co.uk/news/world-us-canada-22883078>> accessed November 2016; US Senate Select Committee on Intelligence *Director of the NSA, General Alexander's remarks to the Senate Intelligence Committee* (18 June 2013)

However, critics of the programme have outlined that it was actually the British Operation Pathway which uncovered Najibullah Zazi's email through a "tip off" rather than PRISM,<sup>832</sup> and have highlighted that US citizens have had their communications accessed, even by accident.<sup>833</sup> Even before PRISM's disclosure, the UN Human Rights Special Rapporteur noted that using warrantless and invasive surveillance programmes on the amorphous basis of "national security" to justify their use was of 'serious concern',<sup>834</sup> and created potential human rights violations when using extra-territorial surveillance.<sup>835</sup> Subsequent to these disclosures, a US Judge for the District of Columbia in *Klayman et al. v Obama*<sup>836</sup> ruled that the use of mass surveillance was likely to be unconstitutional. Consequently, these revelations and the UN's points about the extensive use of legislation such as FISA, highlights an imbalance between the need for security and the requirements of privacy in the US. However, as noted earlier, the US passed the USA Freedom Act, which has forced authorisation of bulk metadata collection by the NSA under §215 of the USA PATRIOT Act to lapse, with

---

<[https://fas.org/irp/congress/2013\\_hr/disclosure.pdf](https://fas.org/irp/congress/2013_hr/disclosure.pdf)> accessed June 2018; McCarthy, T. (The Guardian, 18 June 2013) *NSA chief says exposure of surveillance programs has 'irreversible' impact - as it happened* <<http://www.guardian.co.uk/world/2013/jun/18/nsa-chief-house-hearing-surveillance-live>> accessed November 2016.

<sup>832</sup> Pilkington, E. & Watt, N. (The Guardian, 12 June 2013) *NSA surveillance played little role in foiling terror plots, say experts* <<http://www.guardian.co.uk/world/2013/jun/12/nsa-surveillance-data-terror-attack>> accessed November 2016.

<sup>833</sup> Top secret documents have been released to the Guardian Newspaper which also show that the NSA could use the information of US citizens they incidentally collected; Greenwald, G. & Ball, J. (The Guardian, 21 June 2013) *The top secret rules that allow the NSA to use US data without a warrant* <<http://www.guardian.co.uk/world/2013/jun/20/fisa-court-nsa-without-warrant>> accessed November 2016; The Director of National Intelligence, James R. Clapper, admitted on NBC News that the NSA had accidentally eavesdropped a telephone conversation because of an incorrect digit in 2009; NBC (Transcript, 8 June 2013) *Director James R. Clapper interview with Andrea Mitchell, NBC News Chief Foreign Affairs Correspondent* <<http://www.dni.gov/index.php/news-room/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell?tmpl=component&format=pdf>> accessed November 2016.

<sup>834</sup> LaRue, F. (UN Human Rights Council) *Report of the Special Rapporteur on the promotion and protection of the right of freedom of expression, Frank LaRue* (17 April 2013), 15-16, paras. 59-60 <[http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)> accessed November 2016.

<sup>835</sup> *ibid* para. 64.

<sup>836</sup> *Klayman et al. v Obama* Memorandum and Opinion 16 December 2013 Civ. Action No. 13-0851.

bulk surveillance under §702 of FISA due to expire in 2017.<sup>837</sup> Clearly, despite President Obama’s initial statement following the disclosure of PRISM, when he said: “...you can’t have a hundred per cent security and also then have a hundred privacy and zero inconvenience...”,<sup>838</sup> the US is now ensuring that the collection of data is more appropriate and more constitutionally sound – although the Government has previously fought to quash cases of Fourth Amendment breaches by mass surveillance<sup>839</sup> and has also retroactively granted ISPs immunity for domestic surveillance.<sup>840</sup> These steps may also bring the US more into line with international human rights law, as outlined under Article 15 of the Convention on Cybercrime.

Of particular note is the fact that the PATRIOT Act also lowered previous requirements of formerly issuing a National Security Letters against a person who was known to have terrorist links, to a broad requirement that the information was “relevant” to a national security investigation.<sup>841</sup> As Donohue notes, many NSLs were issued to libraries, schools and companies and even Las Vegas hotels on matters which did not concern terrorism or terrorism-related offences.<sup>842</sup> Donohue further explains that, in 2003, the then Attorney General, John Ashcroft, withdrew a 1995 requirement

---

<sup>837</sup> Singh Guliani, N. (ACLU Legislative Counsel) *What’s Next for Surveillance Reform After the USA Freedom Act* (ACLU Blog, 3 June 2015) <<https://www.aclu.org/blog/washington-markup/whats-next-surveillance-reform-after-usa-freedom-act>> accessed November 2016.

<sup>838</sup> Wall Street Journal *Transcript: Obama’s remarks on NSA controversy* (Blog, 7 June 2013) <<http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/>> accessed November 2016.

<sup>839</sup> *Jewel v. NSA* 673. F. 3d 902 (Ct.App, 9<sup>th</sup> Cir. 2011); No C 08-cv-4373 VRW, MDL No C 06-1791 VRW, No C 07-0693 VRW (Dist.Ct. N.D. CA January 10 2010; *Clapper v. Amnesty International* 133 S. Ct. 1138 (2013), *Center for Constitutional Rights v. Obama* 3:07-cv-01115-VRW (N.D. Cal.) (2011).

<sup>840</sup> Draper, S. *Retroactive Immunity: A Legislative Faux Pas?* (2009) *BYU Prelaw Review*, Vol. 23, 70-71.

<sup>841</sup> Lodgson, K.R. *Who knows you are reading this? The United States’ domestic electronic surveillance in a post-9/11 world* (2008) *Journal of Law Technology & Policy* 409, 420.

<sup>842</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 237.

for the FBI to destroy information gathered in NSLs which were irrelevant to the investigation.<sup>843</sup> Therefore, the appropriateness of NSLs has been criticised, most notably in the case of *Doe v Ashcroft*,<sup>844</sup> whereby it was held that compulsory requests of secret and unreviewable information under the USA PATRIOT Act were contrary to the Fourth Amendment as it “*effectively bars or substantially deters judicial challenges as to the propriety of an NSL request*”.<sup>845</sup> Furthermore, in *ACLU v Gonzales*,<sup>846</sup> regarding NSLs served on libraries, it was found that NSLs were still being used to order information from ISPs while imposing a gagging order on the recipient not to disclose that they had received one.<sup>847</sup> As the court decided, this was a breach of the First Amendment right of freedom of speech.<sup>848</sup> Lodgson noted that the original USA PATRIOT Act was likely to fail two of the objectivity criteria set out in *Freedman v Maryland*,<sup>849</sup> which was meant to limit government censorship and balance any discretion the government may have when limiting freedom of speech.<sup>850</sup> Consequently, the use of simultaneous gagging orders with NSLs has generated some concern that the government is able to overstep its constitutional limitations, and such actions may also impact on its international co-operation with, for example, the European Union, which has a more stringent view of human rights.

---

<sup>843</sup> *ibid* Donohue, 238.

<sup>844</sup> *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

<sup>845</sup> *ibid* 2; Wyden, R. (Sen.) *Law and Policy Efforts to balance security, privacy and civil liberties in post 9/11 America* (2006) 17 *Stanford Law and Policy Review* 331, 334.

<sup>846</sup> *American Civil Liberties Union v. Gonzales* 04 Cir. 2614 Vm 6<sup>th</sup> September 2007.

<sup>847</sup> *American Civil Liberties Union wins PATRIOT Act dispute on disclosure of national security letters – ACLU v Gonzales* (04 Cir, 2614 Vm) 6<sup>th</sup> September 2007 *Computer Law and Security Report* 2007 23(6) 490-491, 490.

NB. This was decided after the law on NSLs was amended in the USA PATRIOT Reauthorisation Act 2006.

<sup>848</sup> *ibid*. The case of *Doe v. Ashcroft* was finally resolved in *Doe v. Holder* S.D.N.Y. 04 Civ. 2614 (VM) (direct) (2010), whereby in a 2010 out of court settlement, the FBI lifted its gagging order against Nicholas Merrill, the Internet Service Provider who challenged the use of NSLs.

<sup>849</sup> *Freedman v. Maryland*, 380 U.S. 51, 58-59 (1965).

<sup>850</sup> Lodgson, K.R. *Who knows you are reading this? The United States' domestic electronic surveillance in a post-9/11 world* (2008) *Journal of Law Technology & Policy* 409, 426.

However, the USA PATRIOT Improvement and Reauthorisation Act of 2006 amends this “gagging” provision, stating under §2709(c) that NSLs should only be prevented from being disclosed when it may endanger national security, interfere with a counterterrorism or criminal investigation or diplomatic relations, or result in danger to life or physical safety of people.<sup>851</sup> Nevertheless, despite this reform, First Amendment rights are still violated due to the fact that NSL recipients are subject to *permanent* gagging orders.<sup>852</sup> Furthermore, the ACLU showed the FBI’s audit exposed a number of serious breaches of power, including NSLs being “*increasingly... used to collect private information... without court approval...*”.<sup>853</sup> Consequently, expansive powers under the PATRIOT Act have been used to gather information on a variety of issues outside terrorism, without consulting US courts. Therefore, using this type of surveillance so broadly is clearly inappropriate and is potentially open to abuse by federal agencies. These concerns are perhaps reflected by the fact that the FBI has recently followed a trend of asking for court orders on limited personal information rather than relying on NSLs,<sup>854</sup> highlighting a more balanced and constitutionally acceptable approach – although perhaps at a cost to immediacy of investigations.

---

<sup>851</sup> 18 U.S.C.A. § 2709(c) (Supp. 2008); *ibid* Lodgson, K.R., 424.

<sup>852</sup> *ibid* Lodgson, K.R., 427; *ibid* *American Civil Liberties Union v. Gonzales* (2007).

<sup>853</sup> American Civil Liberties Union *FBI Audit Exposes Widespread Abuse of PATRIOT Powers* (13 March 2008) <[www.aclu.org/safefree/general/34464prs20080313.html](http://www.aclu.org/safefree/general/34464prs20080313.html)> accessed November 2016; also see the Freedom of Information request in 2007 lodged by the ACLU which highlighted that the Department of Defense had issued NSLs on hundreds of US citizens in which it may have overstepped its legal authority; American Civil Liberties Union *National Security Letters FOIA* (2007) <<http://www.aclu.org/national-security/national-security-letters-foia>> accessed November 2016 and <<http://www.aclu.org/national-security/nsl-documents-released-dod>> accessed November 2016, for further information; *ibid* Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 *Denver University Law Review* 375, 379.

<sup>854</sup> Nakashima, E. (Washington Post, 26 October 2011) *FBI going to court more often to get personal Internet-usage data* <[http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM\\_story.html](http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html)> accessed November 2016; US Department of Justice *Letters from Peter J Kadzik, Principal Deputy Assistant Attorney General, to Harry Reid, Majority Leader, US Senate, Nancy Pelosi, Minority Leader, US House of Representatives, Mitch McConnell, Minority Leader, US Senate, Eric Cantor, Majority Leader, US House of Representatives, John Boehner, Speaker, US House of Representatives, Joseph R. Biden Jr, President, US Senate, and Patrick J. Leahy, Chairman, Committee on the Judiciary* (30

It is clear that, due to the extreme pressures of 9/11, the USA PATRIOT Act was passed quickly without consideration of using wide-ranging powers which also have the ability to be intrusive and potentially capture the communications of innocent Internet users. Moreover, the PATRIOT Act's surveillance measures have been found to violate fundamental Constitutional rights, without proper recourse to judicial or independent oversight. Clearly, to rebalance the requirement of national security with civil liberties, more judicial intervention is needed, as well as independent, periodic monitoring of the use of these powers, to bring this more into line with the US's international obligations under the Cybercrime Convention. Furthermore, instead of Congress continually reauthorising the PATRIOT Act, a full-scale review of the surveillance requirements under Title II is needed to ensure proper checks and balances are maintained and that powers adhere to the Constitution. Moreover, the pen registers and trap and trace devices should also be updated to consider the differences between using these forms of surveillance on telephones and on emails – particularly in redesigning programmes so that only non-content of an email is available to law enforcement until a warrant is issued.

#### **4.3. Legitimate Sources of Finance**

The resulting investigation of the 9/11 Commission found that a number of financial sources of the terrorists involved included using legitimate charities and financial institutions to raise and channel terrorist finances both globally and in a manner which

---

April 2013), 2 <[http://www.justice.gov/nsd/foia/foia\\_library/2012fisa-ltr.pdf](http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf)> accessed November 2016, which explain that in 2012, 15,229 NSL requests were made; in comparison with 16,511 in 2011, *FISA Annual Report to Congress* (30 April 2012): <<http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>> accessed November 2016.

would remain undetected.<sup>855</sup> Therefore, the focus of US federal agencies was to locate such transactions and prevent such legitimate institutions from being used to finance terrorist attacks.

#### 4.3.1. Charities

The 9/11 Report focused on charities with “*corrupt*” employees with sympathies to al-Qaeda, and those who had international reach with “*lax external oversight and inefficient internal controls*”.<sup>856</sup> As Bell notes, charities and non-profit organisations are attractive to terrorist organisations for four main reasons – they are not closely regulated due to tax exemption;<sup>857</sup> their employees are volunteers so there is limited oversight of charitable activities; they retain more money due to their tax-exempt status and they can raise money within the US and send it overseas.<sup>858</sup> Consequently, the PATRIOT Act has a number of measures to identify donors and to increase effective oversight of charitable organisations. With regard to donors, §805(1)(A) of the PA-

---

<sup>855</sup> *ibid* 9/11 Commission Report (22 July 2004), 170-171 <<http://www.9-11commission.gov/>> accessed November 2016; for the hijackers’ use of financial institutions, 9/11 Commission Report (22 July 2004), 237.

NB. It was well known prior to the 9/11 Commission Report and 9/11 itself that some charities were involved in financing terrorist organisations. For example, the U.S. intelligence community received intelligence on the charity al-Haramain Islamic Foundation, some of whose branches were involved in financing jihadists and al-Qaeda. The U.S. had allegedly raised their concerns with the Saudi Arabian Government since 1998; Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*, 12 <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018; the US also monitored the charity Holy Land Foundation for Relief and Development and its financing of the US-designated terrorist organisation, HAMAS, between 1994 and when it blocked the charity’s assets in December 2001; *United States v El Mezain et al.* No. 09-10560 F.3d 2011 WL 6058592 (5th Cir. Dec. 7, 2011), 7; 11.

<sup>856</sup> *ibid* 9/11 Commission Report (22 July 2004), 170 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>857</sup> Under §501(c)(3) of the Internal Revenue Code of 1986 (Pub. L. 99–514, 100 Stat. 2095) (26 U.S.C.) for more information on tax exempt organisations.

<sup>858</sup> Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 Kansas Journal of Law and Public Policy 450, 456.



TRIO Act makes it an offence to provide material support for terrorism, by enhancing and strengthening §2339A and B, Title 18 of the US Code,<sup>859</sup> through increasing maximum penalties.<sup>860</sup> Furthermore, surveillance techniques under Title II of the Act come into force to prove association between donors and terrorist organisations.<sup>861</sup> Charities which intentionally support terrorism, are caught by the PATRIOT Act, which also imposes fines and imprisonment for up to 15 years under §2339A(a).<sup>862</sup> Furthermore, in 2003, a new provision was inserted into §501 of the Internal Revenue Service (IRS) Code to deal with specific sanctions for organisations which are designated as supporters of terrorism.<sup>863</sup> Sanctions under §501(p) include automatic suspension of tax exempt status<sup>864</sup> and denial of charitable deductions on contributions to terrorists or terrorist-affiliated organisations.<sup>865</sup> Moreover, assets of charities suspected of supporting terrorism can be blocked or frozen in times of national emergency under the International Emergency Economic Powers Act of 1977 (IEEPA), Presidential Order 13,224 and §981(1)(G) of Title 18.<sup>866</sup> As Bell explains, the Order does not require knowledge or intent, so a charity can violate the Order *without* knowing it is

---

<sup>859</sup> Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) *Journal of Money Laundering Control* 281, 282.

<sup>860</sup> Crimm, N. *High Alert: The Government's war on the financing of terrorism and its implications for donors, domestic charitable organizations and global philanthropy* (2004) 45 *William and Mary Law Review* 1341, 1405.

<sup>861</sup> *United States v Al-Hussayen* No 03-040 (D. Idaho 2003); Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 *CommLaw Conspectus* 119, 153.

<sup>862</sup> *ibid* Bell, J.L., 459.

<sup>863</sup> *ibid* Bell, J.L., 460.

<sup>864</sup> *ibid*.

<sup>865</sup> *ibid* 406-461.

<sup>866</sup> Ferrari, E. *Deep Freeze: Islamic Charities and the War on Terror* (2004-2005) 7 *Scholar* 205, 210; Al-Marayati, L. *American Muslim Charities: Easy Targets in the War on Terror* 25 *Pace L. Rev* 321, 321; *ibid* Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) *Journal of Money Laundering Control* 281, 282.

NB. The Department of Treasury also publishes *Best Practice Guidelines for charities*, the most recent being in 2010; US Department of the Treasury *Best Practice Guidelines for charities* (2010) <[https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines\\_charities.pdf](https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines_charities.pdf)> accessed April 2018.

supporting terrorism.<sup>867</sup> Despite this being in force for over thirty years, this law was still incredibly effective, as it was estimated that these sanctions, by 2003, froze \$125million in terrorism-related assets worldwide, with approximately \$6.3million assets relating to charitable organisations frozen in 2002.<sup>868</sup> Therefore, after 9/11, the USA PATRIOT Act and existing economic sanctions were strengthened and expanded in order to trace and freeze terrorist finances donated through legitimate sources such as online charities.

However, finding donors and charities intentionally raising finances for terrorist organisations is difficult when terrorist organisations use legitimate charities to disguise their funds, limiting effectiveness, and denying the US the ability to fully achieve the 1999 Convention's aim of preventing the movement of funds suspected to be intended for terrorist purposes.<sup>869</sup> As mentioned in chapter three, in the case of *US v Arnout*,<sup>870</sup> it was found that the charity Benevolence International Foundation transferred and raised funds for al-Qaeda operations over the Internet while using its charitable status as a front.<sup>871</sup> Additionally, terrorists can infiltrate existing charities to

---

<sup>867</sup> Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 Kansas Journal of Law and Public Policy 450, 458.

<sup>868</sup> Crimm, N. *High Alert: The Government's war on the financing of terrorism and its implications for donors, domestic charitable organizations and global philanthropy* (2004) 45 William and Mary Law Review 1341, 1373.

<sup>869</sup> Chapter one, 1.4.2.1.

<sup>870</sup> *United States v. Arnout* 02-CR-892 (N,D, III, 1 November 2002); *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 17.

<sup>871</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 17 and Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 142 (on the Internet); Al-Marayati, L. *American Muslim Charities: Easy Targets in the War on Terror* 25 Pace L. Rev 321, 326; Tibbetts, Lt Col P. S. *Terrorist Use of the Internet and Related Information Technology: A Monograph* School of Advanced Military Studies, Fort Leavenworth (2001-2002), 20  
<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.859.2001&rep=rep1&type=pdf>> accessed June 2018; *ibid* Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) Journal of Money Laundering Control 281, 231 (regarding the case in general).

mask financing, as a proportion of donations would still be channelled into legitimate charitable causes,<sup>872</sup> such as the Holy Land Foundation for Relief and Development in *US v el-Mezain et al*,<sup>873</sup> creating difficulties distinguishing between them and wholly legitimate charities<sup>874</sup> (although both *Arnout* and *el-Mezain* highlight lengthy but successful examples of US prosecution against charities who are used to finance terrorism).

It is also difficult for law enforcement to prove donors knew they were directly providing material support to terrorism,<sup>875</sup> creating concern about both the appropriateness and effectiveness of provisions.<sup>876</sup> Although §2339B, Title 18 USC, creates a criminal offence to materially support one of the organisations listed in Order 13,224, it is difficult to prove intent in “*routine cases*”.<sup>877</sup> Furthermore, online charities can be located *anywhere* in the world, so they may not be subject to such stringent legislation in other jurisdictions.<sup>878</sup> For example, despite Benevolence Foundation being listed as a charity with terrorist links and had its assets frozen in the US, it “*continue[d]*

---

<sup>872</sup> E.g. Benevolence International Foundation; Holy Land Foundation – convictions of the founders in 2009 for terrorism offences, convictions upheld on appeal on 7 December 2011; Case No 09-10560 United States Court of Appeals Fifth Circuit *United States of America v. Mohammad el-Mezain ; Ghassan Elashi; Shukri Abu Baker; Mufid Abdulqader; Abdulrahman Odeh; Holy Land Foundation for Relief and Development*; Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 18; Thomas, 116.

<sup>873</sup> *ibid* *United States v. Mohammed el-Mezain, Ghassan Elashi, Shukri Abu Baker, Mufid Abdulqader, Abdulrahman Odeh, Holy Land Foundation for Relief and Development* No. 09-10560 F.3d 2011 WL 6058592 (5th Cir. Dec. 7, 2011).

<sup>874</sup> *ibid* Hinnen, 18; *ibid* Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 142 ref. Benevolence International Foundation; Baldwin, F.N. *The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?* (2004) 8(2) Journal of Money Laundering Control 127, 130.

<sup>875</sup> Falling within the scope of §2339A, Title 18 US Code – Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) Journal of Money Laundering Control 281, 282.

<sup>876</sup> *United States v Al-Hussayen* CR03-048-C-EJL (D. Idaho 4 March 2004); Chapter 4.2.

<sup>877</sup> *ibid* Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) Journal of Money Laundering Control 281, 283.

<sup>878</sup> *ibid*.

to operate online...” using ISPs located in other countries.<sup>879</sup> Clearly, US legislation becomes less effective when charities operate outside the US and legislative procedures are again compromised by dependence on international co-operation.<sup>880</sup> As a result, a more proactive, rather than reactive, approach may be more effective in tracing terrorist finances generated through online charities. As Bell suggests, a terrorist financing “screening” at the time of a new charity’s s501(c)(3) application with the IRS may therefore be a good preventative measure to implement, heightening effectiveness.<sup>881</sup>

The appropriateness of the current provisions has been criticised for a number of reasons. At a domestic level, firstly, the emergency economic sanctions under IEEPA and the Executive Order have had an adverse effect on legitimate Muslim charities.<sup>882</sup> As Ferrari outlines, post-9/11 legislative instruments risk breaching the First Amendment of the Constitution, or the freedom of religion, through having an indirect impact on Muslim charitable giving, *zakat*.<sup>883</sup> Moreover, as the CRS Report to Con-

---

<sup>879</sup> Tibbetts, Lt Col P. S. *Terrorist Use of the Internet and Related Information Technology: A Monograph* School of Advanced Military Studies, Fort Leavenworth (2001-2002) <<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.859.2001&rep=rep1&type=pdf>> accessed June 2018.

<sup>880</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 19.

<sup>881</sup> Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 Kansas Journal of Law and Public Policy 450, 472-474.

<sup>882</sup> Al-Marayati, L. *American Muslim Charities: Easy Targets in the War on Terror* 25 Pace L. Rev 321, 328; Donohue, L.K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int’l L. 303, 407; 422-425.

NB. It is worth noting that most of the charities listed in the US Treasury’s List of Designated Charities under Executive Order 13,224 are Islamic charities; US Department of the Treasury *List of Designated Charities under Executive Order 13,224* <<http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/designationsum-.pdf>> accessed November 2016.

<sup>883</sup> *ibid* Ferrari, E. *Deep Freeze: Islamic Charities and the War on Terror* (2004-2005) 7 Scholar 205, 214-215; Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 168.

gress outlined as early as 2002, policies used against charities could be seen as implying intolerance against a religious minority.<sup>884</sup> At an international level, as Al-Marayati explains, the effect of indirect religious profiling is that Muslim Americans give less to charities who work internationally,<sup>885</sup> resulting in an adverse effect US anti-terrorist financing legislation has on some overseas aid agencies.

Secondly, the material support provisions under §2339A and B of Title 18 USC have been criticised because the onus is on the donor and charity to prove that they had not known or “should have known” their donations were to be channelled to terrorist organisations<sup>886</sup> which opens them up to liability. As Bell explains, a charity could legitimately provide a block grant to a foreign recipient who then distributes the donations to a number of humanitarian causes, a small percentage of which may have links to terrorism.<sup>887</sup> With such distance between donor and eventual provision, it is unfair that so much focus is placed on the charity to prove it had no knowledge of such a complicated transaction. As Ruff highlights, the pressure of intrusive government investigation and using measures which are overly diligent has caused some charities to cease operations, including KinderUSA.<sup>888</sup> As KinderUSA alleged, although it had

---

<sup>884</sup> Rensselaer, L. RL31658 *CRS Report to Congress Terrorist financing: The US and International Response* (6 December 2002), 5 <[https://www.everycrsreport.com/files/20021206\\_RL31658\\_2009bbd56c90ec7f3a859cef3d688ad17afbf555.pdf](https://www.everycrsreport.com/files/20021206_RL31658_2009bbd56c90ec7f3a859cef3d688ad17afbf555.pdf)> accessed June 2018; Donohue, 422-3.

<sup>885</sup> Al-Marayati, L. *American Muslim Charities: Easy Targets in the War on Terror* 25 Pace L. Rev 321, 328; Ruff, K. *Scared to Donate: An Examination of the effects of designating Muslim charities as terrorist organizations on the First Amendment rights of Muslim donors* (2005) 9 New York University Journal of Legislation and Public Policy 447, 472-475; Ruff also makes an interesting point that Muslim charities who work in a purely domestic capacity may see an increase in funding, 475-476.

<sup>886</sup> Crimm, N. *High Alert: The Government's war on the financing of terrorism and its implications for donors, domestic charitable organizations and global philanthropy* (2004) 45 William and Mary Law Review 1341, 1406-1408; Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 Kansas Journal of Law and Public Policy 450, 460.

<sup>887</sup> *ibid* Bell, J.L., (fn 62); Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 171.

<sup>888</sup> *ibid* Ruff, K. *Scared to Donate: An Examination of the effects of designating Muslim charities as terrorist organizations on the First Amendment rights of Muslim donors* (2005) 9 New York University Journal of Legislation and Public Policy 447, 476-477.

changed its practices to prevent any potential link with terrorist financing, due to surveillance by the US Government, it ceased to solicit donations because “*it could not guarantee to its donors that the federal government would not seize its assets as they had done with many other blacklisted charities*”.<sup>889</sup> Furthermore, as Bell states, due diligence requirements, as set out in the US Treasury’s Guidelines,<sup>890</sup> may also incur onerous and costly requirements on charities through additional staff and grant analysis which some small non-profit organisations would be unable to afford,<sup>891</sup> as well as potentially losing good board members who do not wish to be exposed to PATRIOT Act liabilities.<sup>892</sup> As a result, knowledge and due diligence requirements may have also had an adverse effect on charities which operate within the US and abroad, which will also catch online charities.

However, it is worth noting that arguments based on the unconstitutionality of the material support statutes have tended to fail in front of US courts. In particular, a series of cases brought by the *Humanitarian Law Project*<sup>893</sup> and culminating in *Holder v Humanitarian Law Project*,<sup>894</sup> all discussed the constitutionality of the material support provisions, including freedoms of speech, association and religion under the First

---

<sup>889</sup> *ibid.*

<sup>890</sup> Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 *Kansas Journal of Law and Public Policy* 450, 462; US Department of the Treasury *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S. Based Charities* 2002 (updated in 2006) <[http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines\\_charities.pdf](http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines_charities.pdf)> accessed November 2016.

NB. These are voluntary not mandatory (*ibid* Bell, J.L., 462), although some academics explain that they are attaining a quasi-legal status as the Treasury may see a breach of one of the Guidelines as a breach of fiduciary duty: *ibid* Bell, J.L., 464-465; Crimm, N. *High Alert: The Government’s war on the financing of terrorism and its implications for donors, domestic charitable organizations and global philanthropy* (2004) 45 *William and Mary Law Review* 1341, 1440-1441.

<sup>891</sup> *ibid*; Bell, J.L., 465-466.

<sup>892</sup> *ibid.*

<sup>893</sup> *Humanitarian Law Project v. Reno*, 9 F.Supp.2d 1205 (C.D.Cal. Jun 15, 1998) (No. CV 98-1971 ABC (BQRX)); *Humanitarian Law Project v. Reno*, 205 F.3d 1130 (9th Cir.(Cal.) Mar. 3, 2000) (No. 98-56062, 98-56280); *Humanitarian Law Project v. U.S. Dept. of Justice*, 352 F.3d 382 (9th Cir.(Cal.) Dec. 3, 2003) (No. 02-55082, 02-55083); *Humanitarian Law Project v. Ashcroft* 393 F.3d 902 (2004); *Humanitarian Law Project v. Gonzales*, No. 04-55871 (9th Cir. Apr. 1, 2005).

<sup>894</sup> *Holder v Humanitarian Law Project et al.* 130 S. Ct. 2705 (2010).

Amendment,<sup>895</sup> as well as the “vagueness” of the material support statute.<sup>896</sup> In *Holder v Humanitarian Law Project*, the Supreme Court made its latest decision on a case which had spanned 12 years, holding that §2339B was constitutional and denying challenges under the First and Fifth Amendments.<sup>897</sup> Furthermore, the Supreme Court explained that the material support provisions were sufficiently narrow and clear to preclude vagueness.<sup>898</sup> Moreover, as mentioned previously,<sup>899</sup> the material support provisions do expressly state that it is a criminal offence to materially support terrorism.<sup>900</sup> Consequently, both charities and donors need to have some due diligence with their funds to ensure that they are not caught by the provisions – although this has to be balanced with the unique position that charities hold (due to voluntary employees and tax exempt status) as well as proper monitoring by federal agencies and Government departments. As Bell suggests, it may be worthwhile to have Government intermediaries to monitor charitable grants as well as investigate donations.<sup>901</sup> This would suggest more of a shared obligation to track and trace terrorist financing through charities, going in some part to address concerns about costs and the burdens of due diligence.

#### **4.3.2. Financial institutions**

---

<sup>895</sup> NB. *Holder* also discussed Fifth Amendment rights of due process.

<sup>896</sup> *Humanitarian Law Project v. Ashcroft* 309 F. Supp. 2d 1185, 1192 (CD Cal. 2004), whereby the District Court upheld part of the appeal, explaining that the updated definition of material support to include “expert advice or assistance” under the USA PATRIOT Act was vague.

<sup>897</sup> In fact, the Supreme Court was reflecting what had been decided during all of the previous cases brought by *Humanitarian Law Project*; *Holder* judgement, 5-8.

<sup>898</sup> *ibid Holder* judgement, 15-17.

<sup>899</sup> Chapter four, 4.2.1.

<sup>900</sup> *ibid.*

<sup>901</sup> Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 *Kansas Journal of Law and Public Policy* 450, 467-471.

After the events of 9/11, it was clear that some of the US bank accounts opened by the terrorists were compliant with anti-money laundering (AML) measures under the Bank Secrecy Act of 1970. For example, it was found that the SunTrust Bank accounts used by Mohammed Atta and Marwan al-Shehhi in Florida were all opened using their correct identification documents and dates of birth,<sup>902</sup> and even aroused an internal fraud alert when al-Shehhi had tried to cash a cheque using identification documents with different addresses.<sup>903</sup> Given that al-Shehhi and Atta held a joint bank account and received transactions of \$20,000 and \$70,000, as well as others of \$9,500 and \$10,000 in 2000,<sup>904</sup> this should have automatically triggered Currency Transaction Reports under the Bank Secrecy Act. Yet, without any credible suspicion of wrongdoing, SunTrust failed to do so.<sup>905</sup>

Consequently, the response to terrorist financing channelled through financial institutions after 9/11 was twofold, with the US attempting to reach the 1999 Convention's aims. Primarily, the USA PATRIOT Act outlines mandatory "know your customer" rules, extending "enhanced due diligence" procedures under §312 to correspondent accounts with non-U.S. citizens and banks<sup>906</sup> and identification requirements

---

<sup>902</sup> Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*, 140 <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018 – it is also noted that some of the social security numbers were entered using the hijackers' dates of birth and visa security numbers, but that this was at the tellers' own hands. This also occurred in branches of Bank America in San Diego, as well as local banks such as Hudson United Bank and Dime Savings Bank in New Jersey (ibid); also see Atta's account application and history in *United States v. Zacarias Moussaoui* 591 F.3d 263 (4th Cir. 2010); United States District Eastern District of Virginia *Notable cases United States v. Zacarias Moussaoui Criminal No. 01-455 A* <<http://www.vaed.uscourts.gov/notablecases/moussaoui/exhibits/prosecution/OG00013.pdf>> accessed November 2016.

<sup>903</sup> ibid. The bank had no evidence of criminal activity, therefore did not report it to law enforcement authorities according to the Federal Bureau of Investigation, Federal Bureau of Investigation *FBI's 9/11 Chronology, Part 2 of 2, 158* <<http://vault.fbi.gov/9-11%20Commission%20Report/9-11-chronology-part-02-of-02/view>> accessed November 2016.

<sup>904</sup> ibid Appendix A *The Financing of the 9/11 Plot*, 134.

<sup>905</sup> ibid Appendix A, 141.

<sup>906</sup> Amends §5318 of Title 31 United States Code.



under §326<sup>907</sup> to counteract anonymous accounts. Nevertheless, this may be more difficult to apply with online banking as it is more complicated for law enforcement authorities to trace sources of terrorist finances and eventually stop the flow of money without face-to-face banking or identification.<sup>908</sup> In 2003, the US Government set up the Customer Identification Programme<sup>909</sup> to offset this problem by requiring banks to have a written Customer Identification Programme (CIP), including minimum requirements for special due diligence<sup>910</sup> and customer identification such as name, address, date of birth and social security or passport number of an individual.<sup>911</sup> Furthermore, the CIP guidelines provide for non-documentary identification, including contacting the customer and verifying information from public databases,<sup>912</sup> which can theoretically be applied to online bank accounts. Nonetheless, it is again problematic for law enforcement to find the identity of an account holder, especially if they have provided false information,<sup>913</sup> which limits effectiveness of preventing and counteracting movements of funds suspected to be intended for terrorist purposes.<sup>914</sup>

However, the PATRIOT Act also provides law enforcement authorities with a number of surveillance techniques to counteract the anonymity of the Internet. For example, §505 of the Act allows law enforcement to access previously sensitive information such as financial records by amending the Fair Credit Reporting Act and the

---

<sup>907</sup> *ibid.*

<sup>908</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 29.

<sup>909</sup> *ibid.*; Under Title 31 Code of Federal Regulations B Ch. I Part 103, now Title 31 Chapter X CFR §1020.220: <<http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=b6f067691197ff726a20c3a2046ff3cc&rgn=div8&view=text&node=31:3.1.6.1.4.2.5.3&idno=31>> accessed November 2016.

<sup>910</sup> *ibid* §1010.600.

<sup>911</sup> *ibid* §102.220(a)(2)(i).

<sup>912</sup> *ibid* §102.220(a)(2)(ii)(B)(1).

<sup>913</sup> *ibid* Hinnen, 29.

<sup>914</sup> Chapter one, 1.4.2.1.

Financial Right to Privacy Act to apply to domestic transactions.<sup>915</sup> Additionally, §210 of the PATRIOT Act extends the type of information Government agencies are able to access to bank records and credit card numbers.<sup>916</sup> Therefore, the PATRIOT Act has proactive measures which potentially enable effective investigation and prevention of terrorist financing.

The PATRIOT Act further strengthens the system of Suspicious Activity Reports (SARs)<sup>917</sup> by amending the Bank Secrecy Act under §351. For instance, the amount triggering a SAR is lowered to \$5,000 if formal banking institutions are suspicious by the transaction,<sup>918</sup> although this is not mandatory. Furthermore, civil and criminal penalties are imposed on financial institutions which fail to comply with having a SARs system or with reporting requirements.<sup>919</sup> Moreover, §6302 of the Intelligence Reform and Terrorism Prevention Act 2004 states that the Secretary of the Treasury is allowed to prescribe regulations for reporting requirements of “*certain cross-border electronic transmittal of funds*”<sup>920</sup> to help detect and prevent suspicious electronic funds and wire transfers flowing through US borders.<sup>921</sup> Nevertheless, these provisions do not sufficiently take into account the practice of ‘smurfing’, or depositing small amounts of cash in financial institutions, under the set amounts of \$10,000 and \$5,000, which undermines their effectiveness. With online banking, such small deposits are virtually untraceable within billions of transactions which occur

---

<sup>915</sup> Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375, 393-4.

<sup>916</sup> *ibid* Mell, P., 395.

<sup>917</sup> §5318 Title 31 U.S.C.

<sup>918</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 30.

<sup>919</sup> §1010.820 Title 31 Chapter X CFR (civil penalties) and §1010.840 (criminal penalties).

<sup>920</sup> US Department of the Treasury & FinCEN *Feasibility Study of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* (October 2006), 1 <[www.fincen.gov/news\\_room/rp/files/CBFTFS\\_Complete.pdf](http://www.fincen.gov/news_room/rp/files/CBFTFS_Complete.pdf)> accessed November 2016.

<sup>921</sup> *ibid*.

annually,<sup>922</sup> making it more difficult for law enforcement authorities to prevent and counteract the movement of funds.<sup>923</sup>

The focus on SARs as a means to seek out terrorist transactions is also questionable at best. After 9/11, it was found that the requirements for formal financial institutions to report transactions over \$10,000<sup>924</sup> were bypassed by the 9/11 terrorists, who opened twenty four accounts in four separate banks, depositing between \$3,000 and \$5,000 in each,<sup>925</sup> all without social security numbers.<sup>926</sup> As Roth et al. state, “[t]he 19 hijackers hid in plain sight: none of their transactions could have revealed their murderous purpose, no matter how hard the banks looked at them.”<sup>927</sup> Depositing small, regular amounts<sup>928</sup> into various accounts highlights the differences from finding transactions for money laundering purposes. With money laundering, patterns of suspicious activity can be detected by both money laundering analysts and computer software which can catch unusual transactions and on an individual’s account,<sup>929</sup> whereas this is not the case for terrorist financing. As Donohue mentions, “...it is

---

<sup>922</sup> Over one third of Americans alone used online banking by 2010; Intuit *One Third of Consumers Now Using Online Banking Tools To Manage Finances* (19 October 2010) <[http://about.intuit.com/about\\_intuit/press\\_room/press\\_release/articles/2010/OnlineBankingToolsToManageFinances.html](http://about.intuit.com/about_intuit/press_room/press_release/articles/2010/OnlineBankingToolsToManageFinances.html)> accessed November 2016; this author has worked out that a third of the US population equates to over 104million out of a total of 313million US citizens; US Census Bureau *Census* <<http://www.census.gov/main/www/popclock.html>> accessed 16 February 2012; in 2011, it was estimated that there were over 65 million online “liquid deposit accounts” (savings, checking and money market accounts) in the US alone and that 66% of US Internet users paid their bills online; ComScore *2011 State of Online Banking and Mobile Services* (February 2012) <[http://www.comscore.com/Press\\_Events/Presentations\\_Whitepapers/2012/2011\\_State\\_of\\_Online\\_and\\_Mobile\\_Banking](http://www.comscore.com/Press_Events/Presentations_Whitepapers/2012/2011_State_of_Online_and_Mobile_Banking)> accessed November 2016.

<sup>923</sup> Chapter one, 1.4.2.1.

<sup>924</sup> The Financial Recordkeeping and Currency and Transactions Reporting Act of 1970 (“Bank Secrecy Act”) (Pub. L. 91-508, 84 Stat. 1118) 31 U.S.C. §5313.

<sup>925</sup> Bantekas, I. *Current Developments: The International Law of Terrorist Financing* (2003) 97 American Journal of International Law 315, 321.

<sup>926</sup> *ibid.*

<sup>927</sup> Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission*, 56 <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018.

<sup>928</sup> Also known as ‘smurfing’, which is a money laundering technique – see paragraph above and Chapter three, 3.2.1.

<sup>929</sup> *ibid* Roth et al., 55.

*difficult, if not impossible, to discern patterns in financial transactions that would signify terrorist activity... ”.*<sup>930</sup> Consequently, the use of SARs and placing the burden on financial institutions to trace potential terrorist finances is potentially ineffective as they may seem like any other ordinary transaction.

A further weakness in the SAR system is emphasised through the sheer quantity of reports sent every year to FinCEN, the US’s Financial Intelligence Unit. This creates uncertainty about the effectiveness of existing legislation when applied to online banking. As mentioned before, the PATRIOT Act had endorsed and encouraged reporting requirements on financial institutions. Nevertheless, the resulting investigation of 9/11 highlighted that Government authorities failed to locate suspicious activity on transactions relating to the attacks.<sup>931</sup> As Levitt states, “[a] *painful footnote... is that while some of the hijackers’ transactions were sufficiently suspicious to warrant reporting, none of those reports reached the proper authorities until after 9/11 because of the inefficiency of the reporting system... ”.*<sup>932</sup> Between 1996 and 2003, approximately one million SARs in total were filed to FinCEN,<sup>933</sup> compared with the years between 2003 and 2011, when nearly 10 million SARs were filed with FinCEN.<sup>934</sup> Annual filing also soared from 507,217 in 2003<sup>935</sup> to 1.7 million in

---

<sup>930</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 345 – who also mentions that the Financial Action Task Force also reached the same conclusion in 2002, (fn 55).

<sup>931</sup> Levitt, M., *Stemming the Flow of Terrorist Financing: Practical and Conceptual Challenges* (2003) 27 *Fletcher Forum of World Affairs* 60, 64.

<sup>932</sup> *ibid.*

<sup>933</sup> *FinCEN By the Numbers Report* Issue 16 (May 2011), 4 <<https://www.fincen.gov/news-room/sar-technical-bulletins>> accessed April 2018.

NB. The year 2003 is mentioned as this was the first time terrorist financing was introduced as a check box in the SAR form. Now FinCEN uses “SAR Stats” which is an interactive tool FinCEN *SAR Stats* <[https://www.fincen.gov/news-room/sar-technical-bulletins?field\\_date\\_release\\_value=&field\\_date\\_release\\_value\\_1=&field\\_tags\\_sar\\_report\\_target\\_id=687](https://www.fincen.gov/news-room/sar-technical-bulletins?field_date_release_value=&field_date_release_value_1=&field_tags_sar_report_target_id=687)> accessed April 2018.

<sup>934</sup> *FinCEN By the Numbers Report* Issue 17 (May 2012), 4 <<https://www.fincen.gov/news-room/sar-technical-bulletins>> accessed April 2018 - the actual number is 9,849,540.

<sup>935</sup> *ibid.*

2014,<sup>936</sup> with 916,709 filed in the first six months of 2015.<sup>937</sup> Clearly, this shows that, despite being unable to cope with the amount of SARs before 9/11, US legislation has actually *increased* the burden of finding terrorist finances upon FinCEN and is exposing the possibility that they will be missed again. As Gouvin states, “...*sifting through and making sense of all the financial data that comes to FinCEN is a Herculean task and one which has not been successfully executed in the past...*”.<sup>938</sup> Consequently, this again creates an almost impossible task for law enforcement agencies to locate and eventually freeze terrorist finances.

Despite the potential ineffectiveness of the SARs regime, FinCEN has attempted to alleviate some of the burdens placed on financial institutions, including cost.<sup>939</sup> For instance, in 2009, FinCEN increased the availability of exemptions from filing CTR.<sup>940</sup> Moreover, FinCEN has introduced e-filing for SARs. According to

---

NB. The number of counter terrorist financing SARs had dropped in 2011 from the previous year (ibid at p5 – explaining that terrorist financing SARs had dropped by 14% to 609 out of 794,710 for Depository Institutions).

<sup>936</sup> FinCEN SAR Stats Technical Bulletin (October 2015), 2 <[https://www.fincen.gov/news\\_room/rp/files/SAR02/SAR\\_Stats\\_2\\_FINAL.pdf](https://www.fincen.gov/news_room/rp/files/SAR02/SAR_Stats_2_FINAL.pdf)> accessed April 2018- the true number is 1,726,971.

<sup>937</sup> ibid.

<sup>938</sup> ibid Gouvin, E.J. *Bringing out the big guns: The USA PATRIOT Act, Money Laundering and the war on Terrorism* (2003) 55 Baylor Law Review 956, 974; FinCEN *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System* (2006), 31 <<https://www.fincen.gov/reports-congress-0>> accessed June 2018.

<sup>939</sup> E.g. the Federal Reserve estimated that institutions it regulated filed 90,397 SARs between 2010 and 2011 and, out of this number, 90,397 hours were spent on filing SARs, resulting in a total cost to the taxpayer of \$4,054,305; Federal Reserve Bank *Supporting Statement for the Suspicious Activity Report by Depository Institutions*, 4 <[http://www.federalreserve.gov/reportforms/formsreview/FR2230\\_20120720\\_omb.pdf](http://www.federalreserve.gov/reportforms/formsreview/FR2230_20120720_omb.pdf)> accessed November 2016.

NB. The Federal Reserve Bank, however, supported the continuance of SARs, describing the costs associated with them as “negligible” (ibid). For overall concerns about Title III compliance, Odoyo provides an example of BankAtlantic who paid \$5million in 2004 to fix problems with USA PATRIOT Act compliance and that it feared it would have to pay \$41million for one subsidiary and \$50million for another to fix these problems; Odoyo, S. *The Effects of US Counter-terrorist laws on International Business and Trade* (2010-2011) 38 Syracuse Journal of International Law and Commerce 257, 275.

<sup>940</sup> FinCEN *Annual Report 2010*, 10; 20-21 <[http://www.fincen.gov/news\\_room/rp/files/annual\\_report\\_fy2010.pdf](http://www.fincen.gov/news_room/rp/files/annual_report_fy2010.pdf)> accessed November 2016.

FinCEN, the Electronic Filing System increases timeliness,<sup>941</sup> allowing information to be dealt with quickly<sup>942</sup>, and is said to be much cheaper to file than paper SARs.<sup>943</sup> Consequently, this provides some leeway for financial institutions to keep up with the requirement to file and process SARs. Furthermore, in September 2010, FinCEN proposed a rule to require financial institutions and money services businesses to produce records of cross-border electronic funds.<sup>944</sup> This is intended to provide law enforcement with information on “first in”, “last out” financial institutions and can be requested on transactions of over \$1,000, potentially increasing effectiveness of investigations. However, this is yet to be implemented.

In order to increase its effectiveness, it would therefore be worthwhile for the US to move away from applying existing anti-money laundering techniques to counter-terrorist financing. As mentioned in chapter three, the offences of money laundering and terrorist financing are inherently different – with terrorist financing often referred to as “reverse money laundering”, as it uses legitimate finances for an illegitimate purpose.<sup>945</sup> Consequently, both crimes require alternative approaches by law enforcement.<sup>946</sup> As Roth et al. suggest, it may instead be more effective if law enforcement authorities cooperate with banks and financial institutions to quickly receive transaction records of suspected terrorists in order to trace them before the act is

---

<sup>941</sup> FinCEN *Annual Report 2011*, 62 <[https://www.fincen.gov/sites/default/files/shared/annual\\_report\\_fy2011.pdf](https://www.fincen.gov/sites/default/files/shared/annual_report_fy2011.pdf)> accessed April 2018.

<sup>942</sup> *ibid* – e-filed SARs forms are available for law enforcement authorities to access within two days as opposed to eleven with paper SARs.

<sup>943</sup> FinCEN *FinCEN's reports going paperless* (24 February 2012) <[http://www.fincen.gov/news\\_room/nr/html/20120223.html](http://www.fincen.gov/news_room/nr/html/20120223.html)> accessed November 2016.

<sup>944</sup> Federal Register, Vol. 75, No. 189 (30 September 2010) <<http://edocket.access.gpo.gov/2010/pdf/2010-24417.pdf>> accessed November 2016.

NB. This has not been made into a rule yet – it is still on FinCEN's pending rulemaking list. FinCEN *Pending Rulemaking* <<https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/pending-rulemakings>> accessed April 2018.

<sup>945</sup> Chapter three, 3.2.

<sup>946</sup> *ibid*.

committed.<sup>947</sup> As further surmised by Roth et al, although this would not have prevented 9/11, with increased co-operation between law enforcement and financial institutions under §314 of the PATRIOT Act, this is already a viable option. Indeed, the FBI already has this type of system in place for emergencies.<sup>948</sup>

Regarding the appropriateness of such measures, the court in *United States v Miller*<sup>949</sup> held that there was *no* reasonable expectation of privacy when financial records are held by a bank or third party, therefore the Fourth Amendment right of privacy does not apply.<sup>950</sup> As a result, concerns about law enforcement agency access can only be limited to this judgement. Nevertheless, the Privacy Act of 1974 under §552(a)<sup>951</sup> establishes a Code of Practice for federal agencies to use, limiting access to and disclosure of private records under §552(a)(d) and (b) respectively, with civil and criminal penalties levied against employees who breach the Act.<sup>952</sup> Additionally, the Right to Financial Privacy Act of 1978<sup>953</sup> prohibits government access to financial records unless in certain circumstances,<sup>954</sup> such as customer authorisation,<sup>955</sup> an administrative subpoena,<sup>956</sup> search warrant<sup>957</sup> or judicial subpoena.<sup>958</sup> Consequently, it

---

<sup>947</sup> *ibid*; Roth, Greenberg and Wille, 58-59 – they use the examples of the 9/11 hijackers Nawaf al Hazmi and Khalid al Mihdhar who were known by Government agencies to have bank accounts in New Jersey in August 2001, as well as using debit cards to buy their flights on Flight 77.

<sup>948</sup> *ibid* 59-60.

<sup>949</sup> *United States v. Miller* 425 U.S. 435, 442 (1976).

<sup>950</sup> *ibid* FinCEN *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System* (2006), 23 <<https://www.fincen.gov/reports-congress-0>> accessed June 2018; Baldwin, F. N., 128-9.

<sup>951</sup> Privacy Act of 1974 (Pub.L. 93-579, 88 Stat. 1896) 5 U.S.C. §552(a); *ibid* FinCEN *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System* (2006), 23-25 <<https://www.fincen.gov/reports-congress-0>> accessed June 2018.

<sup>952</sup> §552(a)(g) for civil remedies and §552(a)(i)(1) for criminal penalties – it is treated as a misdemeanour, with employees fined up to \$5,000.

<sup>953</sup> The Right to Financial Privacy Act of 1978 (Pub. L. 95-630, 92 Stat. 3461) 12 U.S.C. 35, §3401.

<sup>954</sup> *ibid* §3403.

<sup>955</sup> *ibid* §3404.

<sup>956</sup> *ibid* §3405.

<sup>957</sup> *ibid* §3406.

<sup>958</sup> *ibid* §3407.

NB. The exceptions are wide and numerous, limiting financial privacy; Exten, S.E. *Major Developments in Financial Privacy Law 2006: The SWIFT Database incident and updates to the Gramm-Leach-Bailey and Fair Credit Reporting Acts* (2007-2008) 3 I.S.J.L.P. 649, 654 (although her comments are in relation to the SWIFT banking database, which will be discussed below).

appears that the US has a number of safeguards against potential abuse by federal authorities.

However, access to financial records of any Internet user has created concern, with Mell stating that the PATRIOT Act loosens legislative protection of privacy<sup>959</sup> and expands agency access to a wide range of records without judicial review.<sup>960</sup> As Donohue also highlights “*any federal agency can now obtain sensitive and private data without any subpoena or judicial intervention, as long as it is investigating one of some 200 possible offenses [sic]...*”.<sup>961</sup> Therefore, financial institutions are faced with problems in deciding between facing a lawsuit from customers whose financial details have been disclosed to federal agencies and substantial penalties for not doing so.<sup>962</sup> As a result, the USA PATRIOT Act reduces the ability to keep financial information private and raises the risk of abuse.

Perhaps the most controversial example of US government departments and agencies overstepping their authority to access financial records is highlighted in their accessing of the SWIFT database, which held the details of banking customers living in the European Union (EU). In 2006, the New York Times found out that US Treasury Department and the CIA had routinely accessed the SWIFT global banking database without the knowledge of the banks, their customers or the EU, because the SWIFT network was based in the US.<sup>963</sup> While the US maintained it had acted within

---

<sup>959</sup> Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375, 393.

<sup>960</sup> *ibid* 394.

<sup>961</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 167.

<sup>962</sup> *ibid*.

<sup>963</sup> Meyer, J. & Miller, G. *Secret U.S. Program Tracks Global Bank Transfers* (Blog, Common Dreams, 23 June 2006) <[www.commondreams.org/headlines06/0623-06.htm](http://www.commondreams.org/headlines06/0623-06.htm)> accessed November 2016; Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 164-165.



the law by using an administrative subpoena,<sup>964</sup> as SWIFT was incorporated under Belgian law,<sup>965</sup> the EU outlined serious concerns that the US government's actions breached EU data protection laws.<sup>966</sup> Matters reached a head in February 2010 when the European Parliament rejected an EU/US agreement to access the SWIFT database,<sup>967</sup> although it later reinstated the agreement in July 2010.<sup>968</sup> Consequently, the tactics employed by the US to access banking details were questionable and potentially endangered international co-operation with Europe under paragraph 3(c) of Security Council Resolution 1373. The US is also one of the few countries<sup>969</sup> with a full mutual legal assistance treaty on criminal matters with the European Union,<sup>970</sup> but even this has restrictions on the use of personal data.<sup>971</sup> Specifically, Article 4 of the agreement deals with banking information, noting that one of the parties must "*promptly ascertain if the banks located in its territory possess information of whether an identified natural or legal person suspected of or charged with a criminal offence is the holder*

---

<sup>964</sup> Exten, S.E. *Major Developments in Financial Privacy Law 2006: The SWIFT Database incident and updates to the Gramm-Leach-Bailey and Fair Credit Reporting Acts* (2007-2008) 3 I.S.J.L.P. 649, 654.

<sup>965</sup> *ibid.* 651-652.

<sup>966</sup> *ibid.* 657.

<sup>967</sup> BBC News (11 February 2010) *European Swift bank data ban angers U.S.* <<http://news.bbc.co.uk/1/hi/world/europe/8510471.stm>> accessed November 2016.

<sup>968</sup> European Parliament, 11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE) *Legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0279+0+DOC+XML+V0//EN&language=EN>> accessed November 2016.

<sup>969</sup> Japan, Norway and Iceland have mutual legal assistance treaties with the EU as well. European Union 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union ('MLAC') & Protocol - Implementation - Extended to Norway and Iceland 2000/C 197/01 <<http://eur-lex.europa.eu/LexUriServ/LexUriS-erv.do?uri=OJ:C:2000:197:0001:0023:EN:PDF>> accessed April 2018; European Union *Agreement between the European Union and Japan on mutual legal assistance in criminal matters* (European Union, 12 February 2010) <<http://eur-lex.europa.eu/LexUriServ/LexUriS-erv.do?uri=OJ:L:2010:039:0020:0035:EN:PDF>> accessed April 2018.

<sup>970</sup> US Department of State *Mutual Legal Assistance Treaty between the United States of America and the European Union*, (25 June 2003, Entry into force 1 February 2010) <<https://www.state.gov/documents/organization/180815.pdf>> accessed April 2018.

<sup>971</sup> *ibid.* Article 9.

of a bank account or accounts”.<sup>972</sup> However, the wording denotes clearly that this provision of information is based on request, rather than obtaining evidence by back-handed means. As a result, by accessing the database without a request being approved by the European Union, such actions can be held inappropriate under the US’s international agreements. Instead, the US should be seeking to balance security and privacy requirements with its cooperation with outside jurisdictions.

#### 4.4. Cybercrime

The problems encountered by law enforcement officials are compounded by the use of false information and fraudulent activities, masking the transfer of funds used for terrorist activities.<sup>973</sup> For example, cyberlaundering (the laundering of electronic cash through using stored value cards as well as Internet wire transfers),<sup>974</sup> and online credit card fraud provide a simple and effective way of counteracting US cross-border transfer provisions. Since 9/11, the USA PATRIOT Act has included cybercrime on the

---

<sup>972</sup> *ibid* Article 4 (1).

<sup>973</sup> *ibid* Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5.

<sup>974</sup> Weaver, S.J. *Modern Day Money Laundering: Does the solution exist in the expansive system of monitoring and record-keeping regulation?* (2005) 24 Annual Review of Banking and Finance Law 443, 449-452. Cyberlaundering works in the same way as money laundering by using the three stages of placement, layering and integration. Criminals see the Internet as a great advantage for cyberlaundering due to its anonymity and ease of travelling across multiple borders without detection. With regard to e-money, Straub states: “*The cyberlaunderer can evade current anti-laundering tactics by depositing e-money in an Internet bank, without any reporting requirements, because e-money accounts usually operate independent of financial institutions. In addition, e-money affords the account holder complete anonymity to conduct Internet transactions, with virtually no means for identifying the purchaser, because any computer connected to the Internet can access e-money accounts.*” Straub, J.P., *The Prevention of E-money Laundering: Tracking the elusive audit trail* (2001-2002) 25 Suffolk Transnat’l L. Rev. 515, 521.

list of terrorist offences<sup>975</sup> and has added provisions in the Homeland Security Act of 2002, which have significantly increased penalties for computer fraud and abuse.<sup>976</sup>

#### **4.4.1. Cyberlaundering**

In order to combat cyberlaundering, the PATRIOT Act has a number of controls aimed at money laundering, building on existing legislation to carry out a number of techniques which are applicable to Internet transactions.<sup>977</sup> These include enhancing the Bank Secrecy Act's record-keeping and reporting requirements<sup>978</sup> and increasing criminal and civil penalties for individuals and businesses engaged in cyberlaundering,<sup>979</sup> providing strong deterrents. Furthermore, the Act introduced "long arm" jurisdiction over foreign bank records under §317(2),<sup>980</sup> enabling district courts to subpoena records of cyberlaunderers and potential counter terrorist financiers overseas, thus catching global Internet transactions. Additionally, the PATRIOT Act expands the definition of "financial institutions" to include informal value transfer systems and money transmitting businesses,<sup>981</sup> thereby incorporating forms of e-money, such as e-

---

<sup>975</sup> §2332b(g)(5)(B) Title 18 U.S.C; Electronic Frontier Foundation *Analysis of the Provisions of the USA PATRIOT Act that relate to online activities Title III section B* (31 October 2001) <[http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031\\_eff\\_usa\\_patriot\\_analysis.php](http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php)> accessed November 2016 Electronic Frontier Foundation, (31 October 2001) *Analysis of the Provisions of the USA PATRIOT Act that relate to online activities Title III section B* <[http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031\\_eff\\_usa\\_patriot\\_analysis.php](http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php)> accessed November 2016.

<sup>976</sup> Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 24.

<sup>977</sup> E.g. Bank Secrecy Act of 1970.

<sup>978</sup> Hunt, J. *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them* (2011) 20(2) Information & Communications Technology Law 133, 139.

<sup>979</sup> §363 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272).

<sup>980</sup> *ibid* Hunt, J., 139; Turner, S. *US Anti-Money Laundering Regulations: An economic approach to cyberlaundering* (2003-2004) 54 Case W. Res. L. Rev. 1389, 1413.

<sup>981</sup> Through including them in reporting suspicious activities under §359 – definitions under §359(a) and (b); *ibid* Turner, S., 1411-1412; Weaver, S. *Modern Day Money Laundering: Does the solution exist in the expansive system of monitoring and record-keeping regulation?* (2005) 24 Annual Review of Banking and Finance Law 443, 448.

Gold.<sup>982</sup> Moreover, compulsory registration for online services which fall within the definition of a Money Services Business<sup>983</sup> was introduced, meaning that online payment services such as PayPal were brought under the same stringent requirements as formal banking institutions.<sup>984</sup> As a result, the USA PATRIOT Act has a robust outlook on cyberlaundering.

With regard to effectiveness, the US is party to a major international instrument which has been important in combating cybercrime, including cyberlaundering, through ratifying the 2001 European Convention on Cybercrime in 2006.<sup>985</sup> As Vatis notes, the US - although being a Council of Europe observer - had influenced the drafting of this Convention,<sup>986</sup> given that it had more experience in other countries in combatting computer crime.<sup>987</sup> Provisions such as Article 14(2) of the Convention extends the notion of cybercrime to any crime where it is necessary to collect evidence in electronic form,<sup>988</sup> meaning that traditional crimes such as fraud and money laundering committed via the Internet would be caught by the Convention. The Convention is split into three main categories:

---

<sup>982</sup> NB. More about e-Gold will be explained later in this section.

<sup>983</sup> US Department of the Treasury *U.S. National Money Laundering Strategy 2007* Appendix A, 45 <<https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf>> accessed April 2018.

<sup>984</sup> *ibid* Turner, S., 1411 – noting that the US Treasury Department concluded PayPal was an informal money transfer system.

<sup>985</sup> Library of Congress *Congressional Record*, 109th Congress, 2nd Session Issue: Vol. 152, No. 106 — Daily Edition, S8901-S8902 (3 August 2006) <<https://www.congress.gov/congressional-record/2006/08/03/senate-section/article/S8901-2?>> accessed November 2016; Techlaw Journal *Senate Ratifies Convention on Cybercrime* (3 August 2006) <<http://www.techlawjournal.com/topstories/2006/20060803b.asp>> accessed November 2016.

<sup>986</sup> Vatis, M. A. *The Council of Europe Convention on Cybercrime* (2010) Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, 207 <<http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf>> accessed April 2018.

<sup>987</sup> *ibid*.

<sup>988</sup> *ibid* 208.

***Criminal Offences***<sup>989</sup> - including computer-related offences such as fraud,<sup>990</sup> and content-related offences such as child pornography;<sup>991</sup>

***Investigatory powers*** - including data retention,<sup>992</sup> and the interception of data content;<sup>993</sup>

***International co-operation***<sup>994</sup> - including mutual legal assistance and evidence collection.<sup>995</sup>

These three elements, when taken as a whole, enable jurisdictions to work together to provide each other with evidence on all criminal offences committed with the assistance of a computer, which inevitably increases effectiveness, by taking out the ordinary limitations of territorial jurisdiction. As Vatis further explains, while there are no statistics by which to meaningfully compare international co-operation before and after the Convention, the greatest observable increase of its effectiveness has occurred in countries which have ratified the convention in recent years.<sup>996</sup> Where improvements have been seen significantly, is within those of serious investigations where time is of the essence, including co-operation through the ability to require preservation of evidence,<sup>997</sup> the creation of a 24/7 network,<sup>998</sup> and the ability to engage in remote searches.<sup>999</sup> As such, the Convention - which has nearly 60 signatures and

---

<sup>989</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), s. 1 Title II.

<sup>990</sup> *ibid* Article 8.

<sup>991</sup> *ibid* Article 9.

<sup>992</sup> *ibid* Article 16.

<sup>993</sup> *ibid* Article 21.

<sup>994</sup> *ibid* Chapter III.

<sup>995</sup> *ibid* Article 25(1).

<sup>996</sup> *ibid* Vatis, M. A. *The Council of Europe Convention on Cybercrime* (2010) Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, 220 <<http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf>> accessed April 2018.

<sup>997</sup> *ibid*.

<sup>998</sup> *ibid*.

<sup>999</sup> *ibid*.

ratifications -<sup>1000</sup> provides the US with enhanced capabilities of investigating and tracking terrorist finances derived from cybercrime.

Furthermore, under domestic law, the US Department of Justice has a dedicated Computer Crime department,<sup>1001</sup> which has had some success on finding money laundering through money transmittal websites such as e-Gold.<sup>1002</sup> However, as the US Treasury explains, it is difficult to trace finances once Internet users switch from a formal way of banking to an informal online payments system like e-Gold, due to the lack of record-keeping facilities of some ISPs and lack of identification procedures.<sup>1003</sup> Consequently, it is problematic for law enforcement authorities to trace whether cyber-laundering has either happened or been used to fund terrorist acts, therefore weakening the effectiveness of provisions used, which is evidenced by the few high profile cases authorities have brought against cyberlaunderers since e-Gold.<sup>1004</sup>

A key extra-territorial provision of the USA PATRIOT Act is §311, which allows the US Treasury to order domestic financial institutions to take ‘special measures’ against an entity identified as a ‘primary money laundering concern’ in a foreign jurisdiction.<sup>1005</sup> Under §5318A(b) Title 31 U.S.C, special measures include

---

<sup>1000</sup> Council of Europe, Chart of signatures and ratifications of Treaty 185, accessed 13 April 2018.

<sup>1001</sup> US Department of Justice *Computer Crime and Intellectual Property Section* <<https://www.justice.gov/criminal-ccips>> accessed April 2018.

<sup>1002</sup> US Department of Justice *Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges* (21 July 2008) <<http://www.usdoj.gov/opa/pr/2008/July/08-crm-635.html>> accessed November 2016.

<sup>1003</sup> US Department of the Treasury *U.S. National Money Laundering Strategy 2007* Appendix A, 44 <<https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf>> accessed April 2018.

<sup>1004</sup> US Department of Justice: very few high profile cases which involve money laundering only have been brought, although cyberfraud has produced some results; US Department of Justice *Online Fraud* <<https://www.justice.gov/criminal-fraud>> accessed April 2018.

<sup>1005</sup> §311 USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272) – amends Title 31, Chapter 53, Subchapter II US Code by inserting §5318A which states: (a) (1) *IN GENERAL.*—*The Secretary of the Treasury may require domestic financial institutions and domestic financial agencies to take 1 or more of the special measures described in subsection (b) if the Secretary finds that reasonable*

Suspicious Activity Reports and record-keeping of certain transactions,<sup>1006</sup> as well as prohibitions on opening and maintaining certain correspondent accounts.<sup>1007</sup> In 2013, §311 was used when the Costa Rica-based digital currency system<sup>1008</sup> Liberty Reserve was shut down because of its alleged use by money launderers,<sup>1009</sup> and when the US authorities found that 200,000 accounts were held by US customers.<sup>1010</sup> Unlike financial institutions operating online with enhanced customer identification programmes, Liberty Reserve only requested a name, date of birth and email address, and deposits could be made via a third party.<sup>1011</sup> Furthermore, there were no limits on deposit sizes and the service required depositors to use third party exchangers to deposit money,

---

*grounds exist for concluding that a jurisdiction outside of the United States, 1 or more financial institutions operating outside of the United States, 1 or more classes of transactions within, or involving, a jurisdiction outside of the United States, or 1 or more types of accounts is of primary money laundering concern, in accordance with subsection (c).*

<sup>1006</sup> §5318(b)(1), Title 31, U.S.C.

<sup>1007</sup> §5318(b)(5), Title 31, U.S.C.

<sup>1008</sup> NB. Digital or virtual currency is a form of encrypted online currency without government regulation, centralised bank or currency exchange (e.g. Bitcoin). Virtual currency also includes in-gaming currency (e.g. Linden Dollars in the game Second Life) which can be used to purchase online goods but do not have the same legal tender status as ‘real’ currency such as notes or coins. However, virtual currency which can be “convertible” into real currency (such as Bitcoin, an anonymous peer-to-peer digital wallet system which can be converted to ‘real’ currency through Bitcoin exchanges) is the primary concern of US law enforcement authorities as it becomes vulnerable to money laundering; FinCEN *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (18 March 2013) <<https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>> accessed April 2018.

<sup>1009</sup> US Grand Jury Sealed Indictment *United States v. Liberty Reserve S.A. Arthur Budovsky, Vladimir Katz, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jiminez, Azzeddine El Amine, Mark Marmilev and Maxim Chukharev* (2013) S.D.N.Y. 13 Crim 368; Santora, M., Rashbaum, W.K. & Perlroth, M. (New York Times, 28 May 2013) *Online Currency Exchange Accused of Laundering \$6billion* <[http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=2&\\_r=0](http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=2&_r=0)> accessed November 2016.

NB. Liberty Reserve is alleged to have conducted over 55million transactions in seven years, with 1million accounts including those named under “Russia Hackers” and “Hacker Account”; United States Attorney’s Office, Southern District of New York *Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World’s Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A \$6 Billion Money Laundering Scheme* (28 May 2013) <<http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php>> accessed November 2016.

<sup>1010</sup> *ibid* New York Times (28 May 2013).

<sup>1011</sup> *ibid* Sealed indictment 6-7.

thereby limiting customer information<sup>1012</sup> and making it highly attractive to cyber-launderers. As part of a joint two year investigation between 17 countries, including Costa Rica,<sup>1013</sup> this has been widely hailed as a success as the website is now offline. US and Costa Rican authorities have also seized the company's assets<sup>1014</sup> while the defendants have been indicted. The case of Liberty Reserve is actually the first use of §311 of the USA PATRIOT Act against a virtual currency by the US Treasury<sup>1015</sup> and shows the effectiveness of the Act against cyberlaundering, even if currencies are based in foreign jurisdictions.

Despite this success, however, observers note that other virtual currency exchanges are vulnerable to cyberlaundering due to cryptography,<sup>1016</sup> anonymity and ease of evading currency controls.<sup>1017</sup> Subsequent to the Liberty Reserve arrests, many virtual currency exchanges started to adopt anti-money laundering legislation<sup>1018</sup> and, in March 2013, FinCEN designated virtual currency exchanges as money transmitters, meaning that they were subject to anti-money laundering legislation.<sup>1019</sup>

---

<sup>1012</sup> *ibid* 7-8.

<sup>1013</sup> The Costa Rican financial authority Sugef refused to provide Liberty Reserve with a money transmittal licence in 2011 as it had serious concerns about money laundering practices; BBC News (27 May 2013) *Liberty Reserve digital money service forced offline* <<http://www.bbc.co.uk/news/technology-22680297>> accessed November 2016.

<sup>1014</sup> Economic Policy Journal *US Government seizes assets of another Bitcoin Exchange; Firm President Arrested* (28 May 2013) <<http://www.economicpolicyjournal.com/2013/05/us-government-seizes-assets-of-another.html>> accessed November 2016.

<sup>1015</sup> US Department of the Treasury *Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311* (28 May 2013) <<http://www.treasury.gov/press-center/press-releases/Pages/j11956.aspx>> accessed November 2016.

<sup>1016</sup> Forbes Magazine *After Liberty Reserve Shutdown is Bitcoin next?* (31 May 2013) <<http://www.forbes.com/sites/petercohan/2013/05/29/after-liberty-reserve-shut-down-is-bitcoin-next/>> accessed November 2016.

<sup>1017</sup> Kerr, D. (CBS News, 31 May 2013) *Feds don't plan to take down Bitcoin or other currencies* (31 May 2013) <[http://www.cbsnews.com/8301-205\\_162-57587059/feds-dont-plan-to-take-down-bitcoin-or-other-currencies/](http://www.cbsnews.com/8301-205_162-57587059/feds-dont-plan-to-take-down-bitcoin-or-other-currencies/)> accessed November 2016.

<sup>1018</sup> Reuters/CNBC (31 May 2013) *Digital Currency Firms Rush to Adopt Regulations* <<http://www.cnn.com/id/100781308>> accessed November 2016.

<sup>1019</sup> E.g. Record-keeping requirements and identification of customers; FinCEN *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (18 March 2013) <<https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>> accessed April 2018.



Furthermore, in May 2013, another virtual currency exchanger, MtGox had some of its assets frozen and its US-based subsidiary Dwolla<sup>1020</sup> prevented from exchanging currency through it by Homeland Security because it allegedly lied about being a money transmitting business.<sup>1021</sup> As a result, it is clear that the US government is attempting to prevent money laundering through virtual currencies and shutting many of the loopholes available to cybercriminals. However, as a Thomson Reuters White Paper notes,<sup>1022</sup> the new rules do not include virtual currencies exchanged through online gaming.<sup>1023</sup> This, as the White Paper further explains, may be because of the complex nature of regulating online gaming as well as the overwhelming amount of transactions.<sup>1024</sup> For instance, Rosette outlined in 2008, one of the most popular online Massively Multiplayer Online Role-Playing Games (MMORPGs) at the time, Second Life, handled \$400,000 a day in virtual currency and supported over 7,000 businesses,<sup>1025</sup> making it an attractive hub for money launderers. Potentially, therefore, this gap in virtual currency regulation hinders law enforcement authorities and provides terrorist financiers with an easy and anonymous form of laundering money for their aims.<sup>1026</sup>

---

<sup>1020</sup> A start-up based in Des Moines, Iowa; CNET *Homeland Security cuts off Dwolla bitcoin transfers* (14 May 2013) <[http://news.cnet.com/8301-13578\\_3-57584511-38/homeland-security-cuts-off-dwolla-bitcoin-transfers/](http://news.cnet.com/8301-13578_3-57584511-38/homeland-security-cuts-off-dwolla-bitcoin-transfers/)> accessed November 2016.

<sup>1021</sup> *ibid*; see the affidavit served on Dwolla; the owner of MtGox allegedly answered no to questions asking him whether Mutum Silligum LLC, a subsidiary of MtGox, was a money transmitting business when he opened an account with Wells Fargo bank.

<sup>1022</sup> Thomson Reuters *Technology in the fight against money laundering in the new digital currency age* (June 2013) <<https://www.int-comp.org/media/1047/technology-against-money-laundering.pdf>> accessed April 2018.

<sup>1023</sup> *ibid* 14; this is despite the identification by the FBI of online gaming as attractive to money launderer, *ibid* 8; FBI Intelligence Assessment *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity* (24 April 2012) <[http://www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf)> accessed November 2016.

<sup>1024</sup> *ibid*.

<sup>1025</sup> Rosette, D. *The Application of Real World Rules to Banks in Online Games and Virtual Worlds* (2008) 16 U. Miami Bus. Law Rev. 279, 290.

<sup>1026</sup> NB. Linden Lab, which hosts Second Life, has registered as a Money Services Business and began to apply some of the FinCEN guidelines from May 2013 – for instance it has changed its Terms of Service to restrict third party exchangers of its virtual currency to only ‘approved’ exchangers such

Despite the reticence of law enforcement to tackle virtual currency through online gaming, clear steps have been taken by the US to combat money laundering through online gambling, which was identified in 2002 by the FBI as “*a loophole in [the US’s] fight against terrorist financing*”.<sup>1027</sup> Additionally, the United Kingdom case of *R v Tsouli, Mughal and Al-Daour*<sup>1028</sup> highlighted globally that terrorist cells could use online gambling sites to launder money by using stolen credit cards. As Hunt notes, as long as a criminal can open an online account “*that will permit him to set up an account without face-to-face contact or without providing documentary evidence of identity, then it would be extraordinarily difficult for the authorities to trace the account back to the cyberlaunderer...*”,<sup>1029</sup> thereby limiting the effectiveness of law enforcement authorities when finding possible cyberlaunderers and terrorist financiers. Consequently, the US uses the Federal Wire Act of 1961<sup>1030</sup> at §1084(a) to prevent interstate use of wire communications to place wagers or bets, thus catching

---

as LindeX – although this is likely to have been a business decision rather than a legal mandate. See Kadochnikov, A. *Regulatory Classification of the authorized Linden Dollar resellers* (epaylaw, 28 May 2013) <<http://www.epaylaw.com/2013/05/28/regulatory-status-of-linden-lab-and-authorized-linden-dollar-resellers-in-light-of-the-new-terms-of-service/>> accessed November 2016.

<sup>1027</sup> Library of Congress *Congressional Record* 107<sup>th</sup> Congress: V 148 Pt. 13 (September 20 2002 to October 1 2002), 18732 (Representative John LaFalce’s remarks); US House of Representatives Financial Services Committee *FBI Confirms Online Gambling Opens Door To Fraud, Money Laundering; Age Verification Software Ineffective* (3 December 2009) <<http://financial-services.house.gov/News/DocumentSingle.aspx?DocumentID=227740>> accessed November 2016, which notes that the FBI identified online gambling as a vulnerable to terrorist financing; Government Accounting Office, *Internet Gambling: An Overview of the Issues* (December 2002) <<http://www.gao.gov/new.items/d0389.pdf>> accessed November 2016.

<sup>1028</sup> *R v Tsouli, Mughal and Al-Daour* [2007] EWCA Crim 3300 – Younis Tsouli (“irhaby007”), Waseem Mughal and Tariq Al-Daour raised £1.8million to finance a large number of websites and chat rooms which incited acts of terrorism; *Attorney General’s References (Nos.85, 86 & 87 of 2007)*, Re 2007 WL 4368169, [5]; Jacobson, M., *Terrorist Financing and the Internet* (2010) *Studies in Conflict & Terrorism*, 33:4, 353-363, 355.

<sup>1029</sup> Hunt, J., 136.

<sup>1030</sup> Federal Wire Act of 1961 (Pub. L. 87-216, 75 Stat. 491) 18 U.S.C. Part I Chapter 50; Illegal Gambling Business Act of 1970 (Pub. L. 91-452, title VIII) 18 U.S.C. §1955 which applies to offshore gambling businesses taking wagers from US bettors and the Interstate and Foreign Travel or Aid in Racketeering Enterprises Act of 1961 (“Travel Act”) (Pub. L. 87-228, 75 Stat. 498) 18 U.S.C. §1952 prohibiting use of interstate facilities to conduct unlawful business (§1952(a)(1)) including gambling (§1952(b)(1)).

online gambling.<sup>1031</sup> Furthermore, the USA PATRIOT Act also enables the Department of Justice to “*seize any offshore bank account that it believes is engaged in illegal activity, including sheltering the earnings of an internet gambling enterprise*”<sup>1032</sup> and, in 2006, the US took steps to prohibit most online gambling through the introduction of the Unlawful Internet Gambling Enforcement Act<sup>1033</sup> by outlawing any US payment mechanisms being used for Internet gambling under §5363.

Nevertheless, it is questionable whether such prohibitions on Internet gambling are entirely effective or appropriate. For instance, critics such as Weinberg outline that, to outlaw legitimate financial payments mean cyberlaunderers would shift their focus on electronic payment instruments, such as Stored Value Cards, which would not be subject to the same record-keeping requirements as financial institutions.<sup>1034</sup> It has also been said that prohibition, rather than regulation, would drive online gambling to the black market, leading to more fraudulent websites<sup>1035</sup> and creating difficulties for law enforcement agencies to trace transactions which could potentially lead to cyberlaundering or terrorist financing. Moreover, money laundering

---

<sup>1031</sup> Ormand, S., *Pending U.S. Legislation to prohibit offshore Internet gambling may proliferate money laundering* (2004) 10 Law & Bus. Rev. Am. 447, 448-449; *United States v. Cohen* 260 F.3d 68, 68 (2d Cir. 2001) in which it was held that §1084 applied to online gambling (but limited to sports book betting; *In re. MasterCard Int'l Inc.*, 313 F.3d 257, 262-63 (5th Cir. 2002)) and that there were no “safe havens” for offshore gaming sites, 449.

NB. This is Federal law – individual states also have laws prohibiting gambling and Internet gambling – see Weinberg, J. *Everyone’s a Winner: Regulating, not prohibiting, Internet gambling* (2005-2007) 35 Southwest University Law Review 293, 302.

<sup>1032</sup> *ibid* Ormand, S., 449.

<sup>1033</sup> The Unlawful Internet Gambling Enforcement Act of 2006 (Pub. L. 109-347, 120 Stat. 1884) (31 U.S.C. Ch. 53 Subch. IV under Title VIII SAFE Port Act 31 U.S.C. §5361).

<sup>1034</sup> Weinberg, J. *Everyone’s a Winner: Regulating, not prohibiting, Internet gambling* (2005-2007) 35 Southwest University Law Review 293, 294; 313-314 (NB. Although this was written before the UIGEA 2006, the points are pertinent); Boikess, L. *The Unlawful Internet Gambling Enforcement Act: The Pitfalls of Prohibition* (2008) Legislation and Public Policy (12) 151, 183; Government Accounting Office *Internet Gambling: An Overview of the Issues* (December 2002), 34 <<http://www.gao.gov/new.items/d0389.pdf>> accessed November 2016, outlining that credit card experts believed the risks of money laundering would be “heightened” if prohibiting credit card payments was introduced.

<sup>1035</sup> *ibid* Boikess, L., 184.

through online gambling has been claimed to be “quite rare”,<sup>1036</sup> with the FBI only opening two cases on cyberlaundering and online gambling in 2002<sup>1037</sup> (although a number of gambling sites and their owners have been accused of money laundering since, including 34 individuals indicted for money laundering and racketeering by running Legendz Sports in 2013).<sup>1038</sup> Instead, regulation through AML and CTF, as well as record-keeping through credit card transactions, has been mooted as a more effective and appropriate solution for law enforcement.<sup>1039</sup> The UK, for instance, has the Gambling Commission to oversee online gambling and provides guidance on AML and CTF requirements such as customer due diligence and record-keeping.<sup>1040</sup> This

---

<sup>1036</sup> *ibid* Boikess, L., 182-183.

<sup>1037</sup> *ibid* Boikess, L., 182 (fn 195); Government Accounting Office *Internet Gambling: An Overview of the Issues* (December 2002), 35 <<http://www.gao.gov/new.items/d0389.pdf>> accessed November 2016.

<sup>1038</sup> Thomson Reuters *Technology in the fight against money laundering in the new digital currency age* (June 2013), 6 <<https://www.int-comp.org/media/1047/technology-against-money-laundering.pdf>> accessed April 2018; Harris, A. (Bloomberg, 10 April 2013) *Legendz Online Gambling Probe Produces Charges Against 34* <<http://www.bloomberg.com/news/2013-04-10/legendz-online-gambling-probe-produces-charges-against-34.html>> accessed November 2016; United States Attorney’s Office, Western District of Oklahoma *Fifty Seven Charged With Operating Illegal Online Sports Gaming Business* (10 April 2013) <[http://www.justice.gov/usao/okw/news/2013/2013\\_04\\_10.html](http://www.justice.gov/usao/okw/news/2013/2013_04_10.html)> accessed November 2016; NB. Full Tilt Poker owner Ray Bitar also reached a deal with US prosecutors after being charged in 2011 with racketeering and money laundering for running an illegal online betting site; Bowers, S. (The Guardian, 9 April 2013) *Ray Bitar, Full Tilt Founder, strikes deal with US prosecutors* <<http://www.guardian.co.uk/uk/2013/apr/09/ray-bitar-full-tilt-poker-pleads-guilty>> accessed November 2016; United States Attorney’s Office, Southern District of New York. (31 July 2012) *Manhattan U.S. Attorney Announces \$731 Million Settlement Of Money Laundering And Forfeiture Complaint With Pokerstars And Full Tilt Poker* <<http://www.justice.gov/usao/nys/pressreleases/July12/pokersettlement.html>> accessed November 2016. In 2007, Betonsports, a London-based gambling site, pleaded guilty to money laundering and racketeering BBC News (25 May 2007) *Betonsports admits racketeering* <<http://news.bbc.co.uk/1/hi/business/6689813.stm>> accessed November 2016; Clark, A. (The Guardian, 30 September 2009) *Betonsports Chief David Carruthers changes guilty plea in the US* <<http://www.guardian.co.uk/world/2009/sep/30/betonsports-boss-changes-guilty-plea-in-us>> accessed November 2016; and in 2012, the online gambling site PokerStars paid \$731 million after money laundering charges brought against it, *ibid* US Attorney’s Office, Southern District of New York and ABC News (31 July 2012) *PokerStars in \$731M Money Laundering Settlement* <<http://abcnews.go.com/blogs/business/2012/07/pokerstars-in-731m-money-laundering-settlement/>> accessed November 2016.

NB. PokerStars and Full Tilt Poker still operate online.

<sup>1039</sup> *ibid* Weinberg, J. *Everyone’s a Winner: Regulating, not prohibiting, Internet gambling* (2005-2007) 35 Southwest University Law Review 293, 315-316.

<sup>1040</sup> Set up under the Gambling Act 2005 c.19; Gambling Commission *Money Laundering: The Prevention of money laundering and the financing of terrorism – Guidance for remote and non-remote casinos* (December 2011): <<http://www.gamblingcommission.gov.uk/PDF/AML/Prevention-of-money-laundering-and-combating-the-financing-of-terrorism.pdf>> accessed April 2018.

approach perhaps represents a more balanced and effective approach than an outright ban on most online gambling.<sup>1041</sup>

#### **4.4.2. Online Fraud**

As mentioned in chapter three, online fraud can be generated in many different ways, including online auction fraud and credit card fraud.<sup>1042</sup> In 2008, Chargualaf identified auction fraud as the most widespread type of cybercrime,<sup>1043</sup> whereby sellers can misrepresent or not deliver items advertised on sites such as eBay.<sup>1044</sup> In the US, overall Internet crime complaints increased from 50,412 in 2001 to 288,012 in 2015,<sup>1045</sup> with a loss of \$1,070,711,522<sup>1046</sup> to individuals. Out of these statistics, non-auction-non-delivery of merchandise was identified as one of the five top types of Internet crime by the Internet Crime Complaint Center,<sup>1047</sup> highlighting the need of law enforcement agencies to combat this type of cybercrime. Furthermore, online crimes such as credit card and identity theft were identified as ways to support al-Qaeda.<sup>1048</sup> Consequently, it was important for the US to devise strategies to counteract these areas

---

<sup>1041</sup> E.g. Tsouli, Mughal and Al-Daour were found to have opened accounts with stolen credit cards; US House of Representatives Committee on Homeland Security *Written Statement of Andrew R. Cochran For the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing U.S. House Committee on Homeland Security* (31 March 2009) <<https://www.course-hero.com/file/10024718/Counterterrorism-blog/>> accessed November 2016; This author argues that, without legitimate payment mechanisms available to online gamblers, the likelihood of catching Tsouli through stolen credit cards would have been reduced.

<sup>1042</sup> Chapter three, 3.3.1.3.

<sup>1043</sup> Chargualaf, J. *Terrorism and Cybercrime* (Air Command and Staff College, Air University, May 2008), 17 <<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA489730>> accessed November 2016.

<sup>1044</sup> *ibid*.

<sup>1045</sup> Internet Crime Complaint Center (“IC3”) *2015 Internet Crime Report*, 12 <<https://www.ic3.gov/default.aspx>> accessed November 2016.

NB. For the 2001 figures; Internet Crime Complaint Center (“IC3”) *2011 Internet Crime Report*, 6 <[http://www.ic3.gov/media/annualreport/2011\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf)> accessed November 2016.

<sup>1046</sup> *ibid* 12.

<sup>1047</sup> *ibid* – this was the third most reported crime. The other top Internet crimes in the US are business email compromise (1), confidence fraud/romance (2), investment (4) and identity theft (5).

<sup>1048</sup> *ibid* Theohary, C., Rollins, J., *CRS Report to Congress Terrorist Use of the Internet: Information Operations in Cyberspace*, 4.

of cybercrime after 9/11, building on a battery of existing legislation such as the Computer Fraud and Abuse Act of 1986.<sup>1049</sup> For instance, under the USA PATRIOT Act, law enforcement authorities are allowed to require account and credit card details from e-companies under §210, as well as using cross-jurisdictional warrants under §219,<sup>1050</sup> which enable law enforcement authorities to cross jurisdictional boundaries in the US.<sup>1051</sup> Additionally, the Gramm-Leach Bliley Act of 1999<sup>1052</sup> under §6821(b) prohibits the use of false pretences to obtain financial information from a customer.<sup>1053</sup> Although, as Lynch notes, the Act relates to financial institutions, it has been successfully implemented in civil cases,<sup>1054</sup> therefore may have a bearing on cyber fraud investigations.<sup>1055</sup> As regards its effectiveness, there have been some successes, such as the FBI's "Operation Phish Phry"<sup>1056</sup> when 47 were convicted in phishing and identity theft offences in 2009,<sup>1057</sup> and "Operation Ghost Click" in 2011, when six Estonians

---

<sup>1049</sup> Chapter three on the Computer Fraud and Abuse Act of 1986, (Pub. L. 99-174) (18 U.S.C. §1030). For Internet fraud such as auction fraud and phishing, pre-9/11 legislation is used, under Titles 15 and 18 of the US Code including 15 USC §45(a)(1) (unfair or deceptive trade practices), 15 USC §52 (false advertising) (both sections are implemented through the Federal Trade Commission Act of 1914 (Chapter 311, 38 Stat. 717) (15 U.S.C. 41 et seq.)), 18 USC 103(a)(4) (accessing a computer to defraud and obtain something of value (Computer Fraud and Abuse Act of 1986) 18 USC §1956 and §1957 (money laundering through the Money Laundering Control Act of 1986), 18 USC 1343 (wire fraud through the Communications Act of 1934 (Pub. L. 73-416, 48 Stat. 1064) (47 U.S.C. 151 et seq.), added in 1952 under the Amendment Act 1952, Ch. 879, §18(6) 66 Stat 722, 18 USC §1028 (fraud in connection with identity documents and authentication procedures) and §1028A (aggravated identity theft) (both under the False Identification Crime Control Act of 1982, (Pub L. No. 97-398, 96 Stat. 2009) (18 U.S.C 1028, 1738) amended by Identity Theft and Assumption Deterrence Act 1998). For credit card fraud, 18 USC §1030(a)(2)(A) (accessing a computer and obtaining information from a financial institution, card issuer or consumer reporting agency) (Computer Fraud and Abuse Act of 1986), 18 USC §1029 (access device fraud), 18 USC 1343 (wire fraud) and 15 USC §1644 (credit card fraud aggregating at least \$1,000) (through the Truth in Lending Act of 1968 (Pub. L. 90-321 82 Stat. 146) (15 U.S.C. Ch. 41 1601 et seq.)).

<sup>1050</sup> Chargualaf, J. *Terrorism and Cybercrime* (Air Command and Staff College, Air University, May 2008), 21 <<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA489730>> accessed November 2016.

<sup>1051</sup> *ibid.*

<sup>1052</sup> Gramm-Leach Bliley Act of 1999 (Pub.L. 106-102, 113 Stat. 1338) (12 U.S.C.).

<sup>1053</sup> Lynch, J. *Identity theft in Cyberspace: Crime Control Methods and their effectiveness in combating phishing attacks* (2005) 20 Berkley Tech. L. J. 259, 265 fn. 25.

<sup>1054</sup> *ibid* Lynch; *FTC v. Hill* (F.D. Tex. 2004) (No. H 035537).

<sup>1055</sup> NB. There is also a criminal penalty of up to five years' imprisonment under §6823(a).

<sup>1056</sup> Over 100 people were charged in 2009 (50 US citizens and 50 Egyptian citizens) as part of this FBI investigation; Federal Bureau of Investigation *Operation Phish Phry* (7 October 2009) <[http://www.fbi.gov/news/stories/2009/october/phishphry\\_100709](http://www.fbi.gov/news/stories/2009/october/phishphry_100709)> accessed November 2016.

<sup>1057</sup> *ibid.* The ringleader, Kenneth Joseph Lucas II was sentenced to 13 years in June 2011.

were arrested for infecting computers with malware viruses to perpetrate fraud.<sup>1058</sup> In September 2012, however, the Director of the FBI, Robert S. Mueller III, explained to the Senate that the FBI and the legal system had to catch up with technological advances, stating that “[b]ecause of [the] gap between technology and the law, law enforcement is increasingly unable to access the information it needs to protect public safety and the evidence it need to bring criminals to justice..”.<sup>1059</sup> Consequently, from the FBI’s point of view, effectiveness is hampered by the inability of legislation to keep pace with rapidly evolving technology.

Nevertheless, merely updating legislation to correspond with newer technologies is not the only answer to effectively combat cyber-fraud and, in particular, catch potential terrorist financing through this crime. Indeed, as Mr Mueller further states, more partnership and co-operation between law enforcement authorities and ISPs is also needed to be able to counteract cyber-criminals and terrorists.<sup>1060</sup> Most importantly and, as explained earlier, cross-jurisdictional co-operation should be part of an effective plan for jurisdictions such as the US to communicate with ISPs and other jurisdictions’ law enforcement authorities to be able to catch perpetrators of online fraud and terrorist financing in a timely manner. As will be outlined in chapter seven, the United Nations and other international organisations are best placed to ensure that this is a possibility.

---

<sup>1058</sup> Federal Bureau of Investigation *Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business* (9 November 2011) <<https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business>> accessed April 2018.

<sup>1059</sup> Mueller, R.S. *Statement Before the Senate Committee on Homeland Security and Governmental Affairs* (19 September 2012) <<http://www.fbi.gov/news/testimony/homeland-threats-and-agency-responses>> accessed November 2016.

<sup>1060</sup> *ibid.*

#### **4.5. Conclusion**

The US clearly reacted to 9/11 with a battery of new legislation, aimed squarely at CTF and Internet surveillance, as a direct reaction to the use of the Internet by the 9/11 bombers. As the leader in the ‘Financial War on Terror’, it is essential that the US’s measures are both effective and appropriate. Yet, fifteen years later, while some of the provisions of the USA PATRIOT Act were effective in freezing and pinpointing terrorist assets, some of these have had harmful consequences to charities and their donors. Furthermore, the use of the SARs system of identifying suspicious transactions is now cumbersome and outdated. With millions of transactions carried out online daily, applying the SARs scheme would make the task of finding terrorist financing more difficult for law enforcement authorities and financial institutions. It is worth noting, however, that FinCEN has been going further and registering online currencies, so that they are more aware and able to track any potential terrorist use of e-money. These forays into the many uses of the Internet by criminals and terrorists may prove effective in finding their finances. Therefore, while the US has many strengths to its legislation concerning counter-terrorism, it also has many weaknesses.

These weaknesses have been exemplified by the USA PATRIOT Act’s surveillance provisions. The most controversial elements to its reaction to 9/11 were clamping down on foreign intelligence but, through this – whether intentionally or unintentionally - capturing US citizens’ communications and infringing their Constitutional rights. This has proven to be a topic of severe criticism, reaching its pinnacle in 2013, when Edward Snowden revealed the extent to which US law enforcement agencies were using mass surveillance to, essentially, spy on US citizens and a large proportion of Europe. The reaction of the US Government has been to roll back these powers through the Freedom Act 2015, which is meant to stop such techniques by not



renewing §702 FISA. Conversely, without §702, there is the potential that law enforcement will be without a powerful tool to discover terrorist communications, considerably weakening US efforts in its ‘War on Terror’. It therefore remains to be seen whether the Freedom Act will restore the balance between, what is an extremely effective source of information to gather, and the appropriateness of invading its citizens’ privacy rights.

Finally, one key problem hampers the US. Because of its speedy reaction to 9/11, it relied on the existing AML experience it had, rather than viewing CTF as a separate crime altogether. This prevents the US from finding effective and appropriate measures towards finding terrorist finances which are raised and channelled through the Internet and, more significantly, fails to understand that terrorist financing is not necessarily using the financial system to turn dirty money clean, but instead uses the financial system and the Internet to mask the true intentions of where its finances are going – whether dirty or clean. Meanwhile the UK, as outlined in the next chapter, recognises that there are significant differences between CTF and AML, and has therefore formed its legislative strategy to carry out this aim over many years.

## **Chapter Five: The United Kingdom**

*“When young men born and bred in this country, are radicalised and turned into brutal killers...we have to ask some tough questions about what is happening in our country...”*<sup>1061</sup>

### **5.1. Introduction:**

The United Kingdom’s (UK) reaction to the September attacks in 2001 (hereinafter 9/11) and its subsequent legislation has, in many ways, mirrored that of the United States (US). The UK’s reaction to 9/11 was swift, with the rapid introduction of its initial financial sanctions and legislation - much to the dismay of some Parliamentary commentators at the time, who explained that insufficient scrutiny had been afforded to Parliament - <sup>1062</sup> as well as the fact that the UK was the only country to derogate from the European Convention on Human Rights (ECHR) by reasoning that it was a national emergency.<sup>1063</sup> However, despite these concerns, the Anti-terrorism Crime and Security Act 2001 (ATCSA 2001) was introduced within two months of 9/11,<sup>1064</sup> and was enacted on 14<sup>th</sup> December 2001. In particular, the Act expanded on provi-

---

<sup>1061</sup> Former Prime Minister David Cameron, speaking to the House of Commons on the Woolwich terror attack; Cabinet Office *European Council and Woolwich incident: Prime Minister’s statement* (3 June 2013) <<https://www.gov.uk/government/speeches/european-council-and-woolwich-prime-ministers-statement>> accessed November 2016.

<sup>1062</sup> Select Committee on Home Affairs *First Report Anti-Terrorism, Crime and Security Bill* (HMSO, 15 November 2001), paras. 3, 11 <<http://www.publications.parliament.uk/pa/cm200102/cmselect/cmhaff/351/35103.htm>> accessed November 2016.

<sup>1063</sup> NB. The derogation was from Article 5 ECHR (right to liberty). The UK was the only country in the Council of Europe to derogate from Article 5; Parliamentary Joint Committee on Counter Terrorism Policy and Human Rights *Counter Terrorism Policy and Human Rights (Seventeenth Report): Bringing Human Rights Back In* 16th Report of Session 2009-2010, para. 9 (HL Paper 86, HC 111 HMSO, 25 March 2010) <<http://www.publications.parliament.uk/pa/jt200910/jtselect/jtrights/86/8602.htm>> accessed November 2016. The derogation application from Article 5 by the UK Government after 9/11 was held to be valid by the European Court of Human Rights in *A and others v United Kingdom* [2009] ECHR 301 (although the Court held that the measures taken were disproportionate with the derogation in the complainants’ case – this case was specifically dealing with detention under Part Four of the Anti-terrorism, Crime and Security Act 2001 c.24).

<sup>1064</sup> Introduced in Parliament on 19 November 2001.

sions detailed in the Terrorism Act 2000, and dealt with forfeiture of terrorist property,<sup>1065</sup> freezing orders,<sup>1066</sup> as well as the development of data retention to monitor terrorist activities.<sup>1067</sup> Furthermore, the 2001 Act circumvented judicial involvement when freezing assets of non-UK entities,<sup>1068</sup> and expanded open warrants, providing law enforcement authorities with “*the ability to conduct ongoing account monitoring rather than requiring the appropriate officer to seek judicial approval each time [they] sought information related to a terrorist investigation...*”.<sup>1069</sup> Consequently, as with the US, the UK immediately focused on both the finances used by terrorists to further their aims after 9/11.

Although the similarities of the UK and US reactions are clear, instead of a complete *volte-face* towards the financing of terrorism, the UK expanded its existing counter-terrorist financing legislation (CTF) as part of its response to 9/11.<sup>1070</sup> As Donohue noted, 9/11 “*did not so much create new measures as accelerate a process already in motion....*”<sup>1071</sup> Above all, UK legislation treated the financing of terrorism as a separate criminal offence, unlike the US, who had bundled anti-money laundering (AML) and CTF legislation together into one single instrument, the USA PATRIOT Act of 2001.<sup>1072</sup> Therefore, this chapter will compare both the responses of the UK

---

<sup>1065</sup> Anti-terrorism, Crime and Security Act 2001 c.24, Part 1.

<sup>1066</sup> *ibid* Part 2.

<sup>1067</sup> *ibid* Part 3.

<sup>1068</sup> Instead, the UK Treasury could seize an individual’s assets through a statutory instrument, when it reasonably believed a non-UK entity posed a serious threat to the economy; Donohue, L.K. *Anti Terrorist Finance in the United Kingdom and the United States* (2005-2006) 27 Michigan Journal of International Law 303, 343; Anti-terrorism, Crime and Security Act 2001 c.24, Chapter 24, Part I.

<sup>1069</sup> *ibid* Donohue, 343-344.

<sup>1070</sup> Existing CTF legislation included the Prevention of Terrorism Act 1974, c.56 (forfeiture provisions were added in 1976 under the Prevention of Terrorism (Temporary Provisions) Act 1976 (Continuance Order) 1978 SI 1978/487), Part III of the Prevention of Terrorism (Temporary Provisions) Act 1989 c.4, Part IV of the Criminal Justice Act 1993 c.36, the Criminal Justice (Terrorism and Security) Act 1998 and the Terrorism Act 2000 c.11.

<sup>1071</sup> *ibid* Donohue, 344.

<sup>1072</sup> NB. Alexander, R. *Money Laundering and Terrorist Financing: Time for a combined offence* (2009) 30(7) Company Lawyer 200 argues that a combined offence comparable to France’s Code Pé-

and the US under the same areas of directly soliciting donations through websites and email communications, legitimate sources of finance and cybercrime. By comparing and contrasting both countries' legislative responses through case law and comment, this chapter aims to find which response is more effective<sup>1073</sup> and appropriate towards countering the financing of terrorism.

Furthermore, the supremacy of European legislation in this area<sup>1074</sup> has affected the UK's response towards terrorist financing and surveillance, especially since the UK signed the Lisbon Treaty in 2007.<sup>1075</sup> Therefore, it is important within this chapter to discuss European Union (EU) measures in this area, as the UK's compliance both through Regulations and Directives<sup>1076</sup> is juxtaposed with ratification at a UN level.<sup>1077</sup> It is essential to compare whether regional level criminal investigations are

---

nal could make criminal prosecutions more effective (203-204), although notes that fund raising offences under s. 15-16 Terrorism Act 2000 c.11 should remain unchanged as they are clearly separate from money laundering offences.

<sup>1073</sup> NB. The definition of effectiveness here will be through successful prosecutions, as well as examples of successful preventative measures.

<sup>1074</sup> For example, the four Anti-Money Laundering Directives (Directives 91/308/EEC, 2001/97/EC, 2005/60/EC and Directive 2015/849/EU) preside over counter-terrorist financing - although they provide guidance to Member States rather than binding rules.

<sup>1075</sup> 2007/C 306/01 changed the 'pillar' structure of European Union legislation, meaning that criminal matters will be dealt with in the same manner as single market legislation. Specifically, a new Article 4 is inserted, sharing competence with Member States in a number of areas, including freedom, security and justice under Article 4(2)(j). Both EU and national measures in criminal matters are now subject to judicial review by the European Court of Justice; General Secretariat of the Council of the EU *Background: The Lisbon Treaty's impact on the Justice and Home Affairs (JHA) Council: More co-decisions and new working structures* (December 2009) <[http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/111615.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/111615.pdf)> accessed November 2016; Treaty on the Functioning of the European Union (Lisbon Treaty) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:306:0042:0133:EN:PDF>> accessed November 2016.

NB. Under Article 10, Protocol 36, Member States are allowed to opt out of pre-Lisbon Treaty

<sup>1076</sup> NB. It is necessary here to note the difference between Regulations and Directives at EU level as set out in Article 249 of the Treaty Establishing the European Community. A Regulation is a binding legal instrument which must be applied throughout the European Union in its entirety. A Directive sets out the goals of the European Union as well as the parameters of the goal, however, leaves the implementation to individual Member States <<http://europa.eu/eu-law/decision-making/legal-acts/>> accessed November 2016.

<sup>1077</sup> NB. Although Members of the UN are able to sign then ratify Conventions, UN Security Council Resolutions, such as economic sanctions (Article 41 UN Charter), are legally binding under Chapter VII of the Charter of the United Nations <<http://www.un.org/en/documents/charter/chapter7.shtml>> accessed November 2016.

effective and appropriate in this area. The chapter discusses the Data Retention Directive<sup>1078</sup> and data protection implications, as well as comparing the UK's Communications Data Bill to other Member States'<sup>1079</sup> reactions towards communications surveillance and data retention, and the Convention on Cybercrime's focus on data preservation rather than data retention.<sup>1080</sup> This will allow a discussion of whether the UK's move towards more regulated Internet communications is appropriate. Additionally, the chapter investigates the Money Laundering Directives,<sup>1081</sup> in order to assess whether international regulation is able to cope with the intricacies of terrorist financing.

Finally, the chapter assesses the rise of 'cheap terrorism', and investigates whether the UK is able to track and trace small monetary amounts being channelled through the Internet to finance terrorist acts. In particular, the Madrid bombings, the London bombings and both attacks in Boston and Woolwich have highlighted the devastation of cheap terrorism.<sup>1082</sup>

---

<sup>1078</sup> Directive 2006/24/EC (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 <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>> accessed November 2016; in the UK, the Directive is applied through the Data Retention (EC Directive) Regulations 2009 No. 859.

<sup>1079</sup> NB. There will be comparative examples of constitutional cases.

<sup>1080</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Articles 16 and 17.

<sup>1081</sup> The EU currently has four Money Laundering Directives to combat money laundering and terrorist financing at a regional level. They are: Council Directive 91/308/EEC of 10 June 1991; Council Directive 2001/97/EC of 4 December 2001; Council Directive 2005/60/EC of 26 October 2005 and Council Directive 2015/849/EU of the European Parliament and of the Council of 20 May 2015.

<sup>1082</sup> With Madrid, it is estimated that it cost \$10,000 to carry out the attacks, which consisted of thirteen bombs and killed 191 people during the morning rush hour on 11 March 2004; United Nations Security Council S/2004/679 *First report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities* (25 August 2004), 12 <<http://www.un.org/docs/sc/committees/1267/1267mg.htm>> accessed November 2016; the London Underground attacks on 7 July 2005 was estimated to have cost less than £8,000 overall and was self-financed by the bombers; Home Office *Report of the Official Account of the Bombings in London on 7th July 2005* HC1087 (HMSO, 11 May 2006), 23 <<https://www.gov.uk/government/publications/report-of-the-official-account-of-the-bombings-in-london-on-7th-july-2005>> accessed November 2016; after the Boston bombings on 15 April 2013, it was found that Dzhokhar and Tamerlan Tsarnaev used pressure cookers and cheap, low

## 5.2. Direct solicitation of donations

As this is the most overt form of terrorist financing through the Internet, as well as the fact that the majority of Internet users come into contact with email and websites on a daily basis, it is only right that direct solicitation of donations is placed first within the assessment of the effectiveness and appropriateness of the UK's measures.

As mentioned in chapter three, the UK's existing legislative measures contained provisions regarding the direct solicitation of donations both for the donor and the petitioner of donations,<sup>1083</sup> therefore reaching the 1999 Convention's aim to take steps to prevent and counteract the financing of terrorists and terrorist organisations.<sup>1084</sup> The Terrorism Act 2000 already included the offence of inviting another person to provide tangible monetary instruments or property for terrorist purposes under s.15(1)(a), as well as the offence of donating property or money if one knows or suspects it will be used for terrorist activities under s.15(3)(a) and (b).<sup>1085</sup> After 9/11, ATCSA 2001 expanded these measures, allowing freezing orders to be placed on accounts of those suspected in raising terrorist finances<sup>1086</sup> as part of the '*deter, detect*

---

grade explosives to carry out their acts, killing three people and injuring 264; *United States v. Dzhokhar A. Tsarnaev* (District Court of Massachusetts, Case Number: 1:13-cr-10200), [24]-[25], 8 <<http://www.justice.gov/usao/ma/news/2013/April/criminalcomplaint1304211847.pdf>> accessed November 2016. In Woolwich, London, two men, Michael Adebolajo, aka Mujahid Abu Hamza, and Michael Adebolawe, aka Ismail Ibn Abdullah, used knives and cleavers to murder Drummer Lee Rigby on 22 May 2013. The minimal cost of such an act is obvious, as knives and cleavers are available anywhere in the country. *R v Michael Adebolajo (Mujaahid Abu Hamza) and Michael Adebolawe (Ismail bin Abdullah)* Central Crown Court, Sweeney, MJ. *Michael Adebolajo (Mujaahid Abu Hamza) and Michael Adebolawe (Ismail bin Abdullah) 26 February 2014 Sentencing remarks* <<https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/adebolajo-adebolawe-sentencing-remarks.pdf>> accessed June 2018.

<sup>1083</sup> The UK had existing legislation which dealt with contributions to the Irish Republican Army during the 1970s and 1980s, for example, the Prevention of Terrorism (Temporary Provisions) Act 1989 c.4 (repealed). s. 9(1) and (2) made it a criminal offence to make contributions to proscribed terrorist groups; Donohue, L.K. *Anti Terrorist Finance in the United Kingdom and the United States* (2005-2006) 27 Michigan Journal of International Law 303, 331-333.

<sup>1084</sup> Chapter one, 1.4.2.1.

<sup>1085</sup> Terrorism Act 2000 c.11.

<sup>1086</sup> Anti-terrorism, Crime and Security Act 2001 c.24, s. 4-11.

and disrupt’ policies of the UK government against terrorist financing.<sup>1087</sup> Additionally, the Regulation of Investigatory Powers Act 2000 (RIPA) provides law enforcement authorities with the ability to monitor and intercept electronic communications which could be considered as soliciting donations for a terrorist cause. For instance, Part I of RIPA deals with the interception of Internet communications,<sup>1088</sup> including warrants for email addresses<sup>1089</sup> and a duty for communication service providers to assist with a criminal investigation.<sup>1090</sup> Thereby, it catches communications which solicit and provide donations for terrorist activities. Furthermore, Part II of RIPA enables law enforcement authorities to track an individual’s web usage, through obtaining Internet traffic data as part of a criminal investigation.<sup>1091</sup> Therefore, the UK, as with the US, has targeted those who directly solicit funds with aggressive surveillance techniques and financial sanctions following the events of 9/11.

### 5.2.1. Websites

In the immediate aftermath of 9/11, the UK, and the US, realised that websites which openly glorified the attacks were a source of “open intelligence”,<sup>1092</sup> and as Conway

---

<sup>1087</sup> The “deter, detect, disrupt” policies; HM Treasury *Combating the financing of terrorism – A Report on UK Action* (October 2002), 17 <[http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating\\_terrorism.pdf](http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating_terrorism.pdf)> accessed November 2016; Ryder, N. *Financial Crime in the 21<sup>st</sup> Century: Law and Policy* (Edward Elgar, 2011), 78; HM Treasury *Money Laundering Strategy* (October 2004), 13, para. 2.1.; HM Treasury *The Financial Challenge to crime and terrorism* (February 2007) <[http://webarchive.nationalarchives.gov.uk/20120704153538/http://www.hm-treasury.gov.uk/d/financialchallenge\\_crime\\_280207.pdf](http://webarchive.nationalarchives.gov.uk/20120704153538/http://www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf)> accessed April 2018.

<sup>1088</sup> E.g. Regulation of Investigatory Powers Act 2000 c.23, s. 5 provides for interception of communications with a warrant with s. 5(1).

<sup>1089</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 8(2).

<sup>1090</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 11(4)(b) and (c).

<sup>1091</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 21 and s. 22.

<sup>1092</sup> Conway, M. *Terrorist ‘Use’ of the Internet and Fighting Back* (2006) 19 Information & Security 9 <[https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura\\_conway.pdf](https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf)> accessed June 2018, 30, quoting the Staff Statement No. 11 of the 9/11 Commission, 9, which stated that “open sources—the systematic collection of foreign media—has always been a bedrock source of information for intelligence.” *Staff Statement No. 11 of the 9/11 Commission*

pointed out, using the Internet can be a “*double-edged sword*” for terrorists.<sup>1093</sup> Due to the open nature of many websites which solicit donations, it is relatively easy to collate information about individuals who post such sites on the Internet.<sup>1094</sup> Consequently, the UK’s intelligence agency, MI5, posted a number of messages on jihadist websites after 9/11, asking for assistance from potential donors. However, this was hampered by the Federal Bureau of Investigation (FBI) shutting these websites down.<sup>1095</sup> Similar to the US, the UK intelligence agencies also used “honey pots” to lure potential donors into visiting fake websites and disrupting terrorist financing.<sup>1096</sup> Consequently, the UK used essentially the same tactics as the US when dealing with solicitation of donations through websites after 9/11.

However, the UK has gone further than the US in monitoring and shutting down websites which solicit donations for terrorist causes. Under the Terrorism Act 2006, it is a criminal offence to “glorify terrorism”,<sup>1097</sup> thereby catching websites which openly support terrorist activities,<sup>1098</sup> and potentially cutting off donation sources. Therefore, the UK has the ability to prevent the raising of funds through shutting down such websites. Furthermore, the 2006 Act requires Internet Service Providers (ISPs) to remove terrorism-related pages once a notice has been served by

---

<[http://govinfo.library.unt.edu/911/staff\\_statements/staff\\_statement\\_11.pdf](http://govinfo.library.unt.edu/911/staff_statements/staff_statement_11.pdf)> accessed November 2016.

<sup>1093</sup> ibid Conway, M. *Terrorist ‘Use’ of the Internet and Fighting Back* (2006) 19 Information & Security 9 <[https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura\\_conway.pdf](https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf)> accessed June 2018, 29.

<sup>1094</sup> UK Information Commissioner *Study Project: Privacy and Law Enforcement* (February 2004), 27 <[http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/technology\\_and\\_privacy.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/technology_and_privacy.pdf)> accessed November 2016.

<sup>1095</sup> Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 294.

<sup>1096</sup> ibid Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 294; ibid Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 14.

<sup>1097</sup> Terrorism Act 2006 c.11, s. 1(3).

<sup>1098</sup> Terrorism Act 2006 c.11, s. 3.



law enforcement.<sup>1099</sup> However, the effectiveness of shutting down such websites has produced somewhat mixed results. For example, under s.3 (5) and (6), liability is limited if ISPs or content providers have previously made an effort to remove the pages<sup>1100</sup> or are unaware of the offending material.<sup>1101</sup> This stance is reflected by Ofcom, the UK's regulatory body for ISPs, who has been reluctant to enforce security standards onto ISPs,<sup>1102</sup> thereby creating limits for any liability ISPs may have when monitoring extremist websites. Furthermore, in the period between the introduction of the Terrorism Act 2006 and 2009, *no* websites were shut down for terrorism-related content,<sup>1103</sup> and no s. 3 notices had been served in that period.<sup>1104</sup> This highlights the inadequacies of enforcing the Act's provisions regarding website content. It has subsequently been revealed by the former Prime Minister, David Cameron, that between 2011 and 2013, *"5,700 items of terrorist material have been taken down from the internet, and almost 1,000 more items have been blocked...."*<sup>1105</sup> Furthermore, 1,000 extremist websites a week had been taken down by the end of 2015.<sup>1106</sup> However, despite this success, it is unclear whether s. 3 notices have been served during these

---

<sup>1099</sup> Terrorism Act 2006 c.11, s. 3(3). Notices can be served on anyone involved in the provision or use of electronic services such as content providers, content aggregators, hosting ISPs, webmasters, forum moderator or bulletin board hosts and can be served by a "constable" under s. 2(a) (also see Explanatory Memorandum to the Act, [43]).

<sup>1100</sup> Terrorism Act 2006 c.11, s. 3(5)(a).

<sup>1101</sup> Terrorism Act 2006 c.11, s. 3(6)(a).

<sup>1102</sup> House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007), 29 <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016.

<sup>1103</sup> Hope, C. (The Telegraph, 19 March 2009) *Home Office fails to shut down a single extremist website in two years* <<http://www.telegraph.co.uk/news/uknews/defence/5017764/Home-Office-fails-to-shut-down-a-single-extremist-website-in-two-years.html>> accessed November 2016.

<sup>1104</sup> *ibid.*

<sup>1105</sup> Cameron, D. *Oral Statement* (Hansard, 1235, 3 June 2013) <<http://www.publications.parliament.uk/pa/cm201314/cmhansrd/chan10.pdf>> accessed November 2016.

NB. The definition of "terrorist material" in this instance is likely to fall under s. 3(7) and (8) of the Terrorism Act 2006 c.11.

<sup>1106</sup> Mortimer, C. (The Independent, 17 December 2015) *More than 1,000 extremist websites taken down every week London Police Chief Sir Bernard Hogan-Howe says* <<http://www.independent.co.uk/news/uk/crime/more-than-1000-extremist-websites-taken-down-every-week-london-police-chief-sir-bernard-hogan-howe-a6776961.html>> accessed November 2016.

instances. Additionally, with over 1billion websites registered globally by March 2016,<sup>1107</sup> these figures seem comparatively low and therefore the aim of the 1999 Convention to prevent and counteract movements of terrorist funds is not fully realised.<sup>1108</sup> As the Home Affairs Select Committee further noted in July 2013, it was “*deeply concerned that it is still too easy for people to access inappropriate online content, particularly... terrorism incitement...* ”.<sup>1109</sup> It is clear that the UK law enforcement authorities are facing an extremely difficult task in enforcing the related provisions in the Terrorism Act 2006,<sup>1110</sup> as well as the aims of the 1999 Convention.<sup>1111</sup>

Perhaps the most effective results obtained when shutting down websites of this nature have occurred through the efforts of private *hacktivists*, such as the organisation Internet Haganah.<sup>1112</sup> They used Distributed Denial of Service attacks to overwhelm such websites and keep terrorists moving from host to host.<sup>1113</sup> It is clear, that,

---

<sup>1107</sup> NB. Chapter four, 4.2. – the website figures are compiled from Netcraft, who explained that they had received responses to their March 2016 website survey from 1,003,887,790 websites; Netcraft *Web Server Survey* (March 2016) <<https://news.netcraft.com/archives/2016/03/18/march-2016-web-server-survey.html>> accessed November 2016.

<sup>1108</sup> Chapter one, 1.4.2.1.

<sup>1109</sup> Home Affairs Select Committee *E-Crime Fifth Report of Session 2013-14* (HMSO, 17 July 2013), 31, [104] <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>> accessed November 2016.

<sup>1110</sup> Overall, the offences outlined under s. 1 and s. 2 of the Terrorism Act 2006 c.11 tend to be superseded by offences under the Terrorism Act 2000 c.11; Crown Prosecution Service, (5 July 2007) [http://www.cps.gov.uk/news/latest\\_news/137\\_07/](http://www.cps.gov.uk/news/latest_news/137_07/) accessed November 2016; *Attorney General’s References Nos. 85, 86 and 87 of 2007 (Younes Tsouli and Others)*, [2007] EWCA (Crim) 3300, [2008] 2 Cr. App. R(S). 45 (Eng.). Again, Samina Malik (“the lyrical terrorist”) was convicted in 2007 under s. 58 of the Terrorism Act 2000 c.11 because she had stored poetry and terrorist materials on the hard drive of her computer, but this was overturned in *R v Malik* [2008] All ER (D) 201 (Jun) because the prosecution was deemed unsafe.

NB. In *R v Terence Roy Brown* [2011] EWCA Crim 2751 [2012] Cr App R (S.) 10, however, it was held that a conviction on the basis of Brown’s sale of information and CDs on his website which could be of use to terrorists did not breach his Article 10 ECHR rights of freedom of expression and that s. 2 of the 2006 Act (circulation or dissemination of terrorist materials) could not be overridden by Article 10. Brown used the 7/7 bombings as a “selling point” for his CDs and claimed that his sale was purely for financial gain rather than on an ideological basis.

<sup>1111</sup> Chapter one, 1.4.2.1.

<sup>1112</sup> *ibid* Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 295.

<sup>1113</sup> Conway, M. *Terrorism and the Internet: Core Governance and Issues* (2007) 3 Disarmament Forum 23, 31-32; Also mentioned in Ms Conway’s other article *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 294-295.

due to the volume of websites and constraints of time and money of both ISPs and law enforcement,<sup>1114</sup> that some private actors have played a significant role in deciding which websites should be shut down rather than law enforcement agencies. However, the appropriateness of this has been criticised on the basis of subjectivity as to content control employed without state supervision or involvement,<sup>1115</sup> as well as the legality of such acts.<sup>1116</sup> Both intervention of public and private actors have raised concerns about freedom of speech under s.10 of the Human Rights Act 1998,<sup>1117</sup> with critics explaining that the 2006 Terrorism Act “*may serve to stifle legitimate political speech...*”<sup>1118</sup> owing to the subjective nature of shutting down websites. This would also affect the human rights element of Article 15 of the European Convention on Cybercrime, or to provide adequate protection of human rights and liberties.<sup>1119</sup> Consequently, to continue using public-private partnership, the UK has introduced the Counter-Terrorism Internet Referral Unit (CTIRU), enabling ISPs and members of the

---

<sup>1114</sup> Home Office counter-terrorism budgets were protected from budget savings; Home Office *Spending Round: security the foundation of prosperity* says Home Secretary (26 June 2013) <<https://www.gov.uk/government/news/spending-round-security-the-foundation-of-prosperity-says-home-secretary>> accessed November 2016. The Intelligence and Security Committee of the UK Parliament noted that the security intelligence agencies needed to make £220million of savings (*Intelligence and Security Committee Annual Report 2012-13* 36, para. 107). However, both the agencies and the ISC raised concerns about being able to deliver their services while making these savings, 36-38, paras. L and M; Intelligence and Security Committee *Intelligence and Security Committee Annual Report 2012-13* (HC 547) <<http://isc.independent.gov.uk/committee-reports/annual-reports>> accessed November 2016.

NB. In 2013, it was revealed by Edward Snowden that GCHQ, the UK Intelligence Service, was provided with over £100million from the US National Security Agency between 2009 and 2012 to share intelligence gathered from electronic communications; Hopkins, N. & Borger, J. (The Guardian, 1 August 2013) *Exclusive: NSA pays £100m in secret funding to GCHQ* <<http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>> accessed November 2016.

<sup>1115</sup> House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007), 32 <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016.

<sup>1116</sup> Distributed Denial of Service Attacks are criminalised under s. 3(2)(b) of the Computer Misuse Act 1990 (amended by s. 36 of the Police and Justice Act 2006 c.48).

<sup>1117</sup> NB. s. 10 actually goes further than freedom of speech per se, as the European Convention on Human Rights Article 10 confers “freedom of expression”, which includes freedom of speech as well as freedoms surrounding written and broadcast material, as well as published images.

<sup>1118</sup> House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007), 29 <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016.

<sup>1119</sup> Chapter one, 1.4.2.2.

public to report websites contravening counter-terrorism legislation. Reports are then assessed by law enforcement authorities.<sup>1120</sup> Between its inception in February 2010 and 2011, the CTIRU had taken down 93 websites, although the Home Affairs Select Committee noted that none of these websites had been removed using formal terrorism legislation.<sup>1121</sup> However, there has been a significant increase of CTIRU's effectiveness in removing extremist content in partnership with social media websites such as Facebook and Twitter. For instance, between 2010 and 2013, 3,538 pieces of information had been removed, but by December 2013, 18,000 pieces of information had been removed by CTIRU.<sup>1122</sup> By April 2014, CTIRU had removed 29,000 pieces of information relating to terrorist content, including those found on social media websites<sup>1123</sup> and, by 2015, was removing 1,000 pieces of content weekly, 800 of which related to Syria.<sup>1124</sup> However, it is unclear from these statistics how many websites have been removed and whether s.3 notices have been served on individual websites and ISPs. While it is clear on the surface that the CTIRU has become very effective at removing terrorist-related information, it is unclear how the present legislative framework has been used to ensure that its powers and partnership with certain websites and ISPs is also appropriate. Additionally, it is unclear how many websites or

---

<sup>1120</sup> Members of the public can report website content through the [www.directgov.uk](http://www.directgov.uk) website; Home Office *Challenge Online Terrorism and Extremism* (7 April 2011) <<https://www.gov.uk/government/news/challenge-online-terrorism-and-extremism>> accessed April 2018.

<sup>1121</sup> Home Affairs Committee *Memorandum to the Home Affairs Committee Post Legislative Scrutiny of the Terrorism Act 2006* Cm8186 (HMSO, September 2011), [8.1.12], 7 <<http://www.official-documents.gov.uk/document/cm81/8186/8186.pdf>> accessed November 2016.

<sup>1122</sup> Interestingly, there has been a huge increase in removal of pieces of information on websites which relate to terrorism – for instance, CTIRU had applied for approximately 6,500 pieces of information to be removed between 2010 and 2013, with 3,538 pieces removed (Lord Taylor of Holbeach, Parliamentary Under Secretary of State for Criminal Information, *Hansard*, HL Deb (23 September 2013) c421W). This rose to 18,000 pieces by December 2013 (Lord Taylor of Holbeach, HL Deb (12 December 2013) c1003).

<sup>1123</sup> Brokenshire, J. (former Minister for Security and Immigration) *Oral Statement* (Hansard HC Deb c957, 2 April 2014).

<sup>1124</sup> UK National Counter Terrorism Security Office *Online radicalisation* (26 November 2015) <<https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation>> accessed November 2016.

pieces of information which have been removed are have solicited donations for terrorist causes.

Nevertheless, public involvement when reporting such websites can only go so far to disrupt solicitation of donations. As a result, there have been moves towards broader website content filtration, in order to avoid access to the rising tide of extremist websites and contrasting with the voluntary reporting requirements used by the US. At present, the UK already has website filtration, but this is limited to blocking websites which host indecent images of children through the ISP program Cleanfeed.<sup>1125</sup> This is carried out with the assistance of the Internet Watch Foundation (IWF), a private, industry-backed organisation which receives reports from the general public and notifies police and ISPs of illegal website content.<sup>1126</sup> This type of website filtration has proved extremely successful, with 98.6% of such websites being blocked by UK-based ISPs.<sup>1127</sup> In 2012 alone, the IWF took action on 9,550 instances of child sexual content.<sup>1128</sup> However, by the end of 2013, new customers of broadband providers had automatic adult filters in place to block any potentially criminal content and now have to 'opt in' to access such websites. These filters were rolled out to all broadband users at the end of 2014.<sup>1129</sup> Ostensibly to combat child pornography and the accessing of

---

<sup>1125</sup> Illegal websites which show indecent images of children have been blocked since 1996 under the Protection of Children Act 1978, c.37 and with the assistance of the Internet Watch Foundation and ISPs; Internet Watch Foundation *History* <<https://www.iwf.org.uk/about-iwf/iwf-history>> accessed November 2016; British Telecommunications, one of the ISPs serving the United Kingdom, introduced Cleanfeed in 2004, which automatically blocks websites listed by the Internet Watch Foundation as having indecent images of children; Hunter, P. *BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns* (2004) 9 Computer Law and Security 4-5.

<sup>1126</sup> Internet Watch Foundation <<https://www.iwf.org.uk/about-iwf>> accessed November 2016.

<sup>1127</sup> Culture, Media and Sport Committee report *Online Safety Volume I* (13 March 2014), 15, para. 27 (based on written evidence submitted by the Home Office, Ev., 104, para. 10) <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcmums/729/729.pdf>> accessed November 2016.

<sup>1128</sup> Internet Watch Foundation *Annual Report 2012*, 12 <<https://www.iwf.org.uk/report/2012-annual-report>> accessed April 2018.

<sup>1129</sup> Cabinet Office *Rt. Hon. David Cameron Speech to the NSPCC* (24 July 2013) <<https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>> accessed November 2016; BBC News (20 January 2015) *Sky to block pornography by default to protect children* <<http://www.bbc.co.uk/news/technology-30896813>> accessed November 2016.

pornography by under-18s,<sup>1130</sup> it is likely that this filter will extend to extremist websites which support terrorist groups.<sup>1131</sup> Additionally, in November 2013, both Microsoft and Google announced that over 100,000 search terms which will no longer reveal results relating to child abuse imagery and will also contain warnings that child abuse images are illegal.<sup>1132</sup> It is too early to determine whether this type of broad-brush approach will be effective in preventing terrorist websites from being accessed or from soliciting donations. However, this does seem to be a step towards increasing the effectiveness of CTF provisions over the Internet through preventative action.

Despite the potential effectiveness of preventing access to websites which solicit terrorist donations, concerns have already been raised about the appropriateness of the UK's current stance on website censorship, thereby preventing the UK from balancing its actions with the proportionality element of the Cybercrime Convention.<sup>1133</sup> Even Cleanfeed's formation and application have been criticised because of

---

<sup>1130</sup> *ibid.*

<sup>1131</sup> The organisation Open Rights Group has launched a campaign "*Sleepwalking into Censorship*" explaining that the adult filters will encompass extremist websites, as well as other search terms such as alcohol, smoking and web forums and petitioning the Prime Minister to prevent this from happening; Open Rights Group *Sleepwalking into Censorship* (25 July 2013) <<https://www.open-rightsgroup.org/blog/2013/sleepwalking-into-censorship>> accessed November 2016.

<sup>1132</sup> BBC News (18 November 2013) *Google and Microsoft agree steps to block abuse images* <<http://www.bbc.co.uk/news/uk-24980765>> accessed November 2016.

NB. It is important to note that the largest Internet search engines, Google and Microsoft, are clearly making steps towards fundamental website filtration, which could also have implications when dealing with extremist websites.

<sup>1133</sup> Chapter one, 1.4.2.2.

its lack of legislative basis,<sup>1134</sup> leading to concerns about transparency<sup>1135</sup> and leaving the determination of legality to private actors. As Edwards noted, “[t]his censorship needs no laws to be passed, no court to rule... It only needs the collaboration, forced or otherwise, of ISPs”.<sup>1136</sup> Consequently, without this legislative basis or legal oversight, it is difficult to tell whether the ‘opt in’ policy will form a function creep, using technology beyond its original purpose,<sup>1137</sup> into censoring perfectly legal websites, meaning that it “could be the most perfectly invisible censorship mechanism ever invented”.<sup>1138</sup> Furthermore, a number of questions must be raised by the UK Government about this type of website filtration and how information gathered from those who ‘opt in’ would be used as part of a criminal investigation. Clearly, RIPA covers the monitoring of data traffic for national security and criminal investigations<sup>1139</sup> and

---

<sup>1134</sup> Cleanfeed is a private regulator, therefore there is no fundamental legislative framework surrounding its application or for online content filtering; Murray, A. *Information Technology Law: The Law and Society* (3rd Edn. Oxford University Press, 2016), 70-74; Neal, R. (International Business Times, 26 November 2013) *UK Internet Censorship: David Cameron Says Government Will Block 'Extremist' Websites* <<http://www.ibtimes.com/>> accessed November 2016.

NB. Even the Internet Watch Foundation itself is essentially a charity, therefore has no legal right to view images of child sexual abuse (although it has to in order to block the URLs distributing such images) as well as no Parliamentary oversight, it is based on a memorandum of understanding between the Association of Chief Police Officers and the Crown Prosecution Service under s. 46 of the Sexual Offences Act 2003 c.42; Internet Watch Foundation *Memorandum of Understanding* (October 2004) <<https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels/memorandum-of-understanding>> accessed April 2018.

<sup>1135</sup> E.g. The blacklisted sites from the Internet Watch Foundation are not available publicly, therefore there is no way of knowing whether they conform to relevant legislation.

<sup>1136</sup> Edwards, L. *From Child Porn to China*, in *one Cleanfeed* 3(3) SCRIPTed 174 (September 2006), 174 <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1128062](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1128062)> accessed June 2018.

<sup>1137</sup> The definition of function creep can be found at the Dictionary.com as “the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, esp[ecially] when this leads to potential invasion of privacy”; Winner, L. *Autonomous Technology: Technics out-of-control as a Theme in Political Thought* (1<sup>st</sup> Edn. MIT Press, 1977) also defines function creep as using technology for a cause for which it was not originally intended.

<sup>1138</sup> *ibid* Edwards, L..

<sup>1139</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 22 allows law enforcement authorities to obtain communications data in cases of national security (s. 22(2)(a)) or *for the purpose of preventing or detecting crime or of preventing disorder* (s. 22(2)(b)).

the Data Retention (EC Directive) Regulations 2009<sup>1140</sup> required ISPs to retain communications data for a period of 12 months.<sup>1141</sup> As a result, there is the possibility to access data generated from the ‘opt-in’ filters and use it as part of a criminal investigation. However, the details surrounding how these filters will fit into overarching legislation are unclear, as well as how they will be monitored to prevent potential abuse or a function creep towards websites with legal content. For example, Cleanfeed filters blocked a Wikipedia page on a music album after the Internet Watch Foundation placed both the album cover and the page on its blacklist for featuring a suspected indecent image of a person under the age of 18.<sup>1142</sup> The unintended consequences were that UK users of Wikipedia were unable to edit unrelated pages because proxy servers had to be used to access the site.<sup>1143</sup> Although the IWF reversed its decision in December 2008,<sup>1144</sup> citing that it had done so due to contextualising the cover, the potential problems of using a computerised filtration system without such contextualisation are apparent.<sup>1145</sup>

---

<sup>1140</sup> Data Retention (EC Directive) Regulations 2009 SI 2009/859.

NB. Directive 2006/24/EC (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 was declared invalid by the judgement of the Court of justice of the European Union in Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221, which will be discussed at length under chapter five, 5.2.2.

<sup>1141</sup> Data Retention (EC Directive) Regulations 2009 SI 2009/859, s. 4 creates the mandatory requirements for ISPs to retain data and s. 5 creates the requirement to retain the data for 12 months.

<sup>1142</sup> On 5 December 2008, the Internet Watch Foundation blocked a page about the German rock group Scorpions and their album cover “Virgin Killers”, which resulted in Cleanfeed blocking the page; Beaumont, C. & Martin, N. (The Telegraph, 10 December 2008) *Wikipedia ban lifted by Internet Watch Foundation* <<http://www.telegraph.co.uk/technology/news/3700396/Wikipedia-ban-lifted-by-Internet-Watch-Foundation.html>> accessed November 2016.

<sup>1143</sup> Dutton, W.H., Dopatka, A. Hills, M., Law, G & Nash, V. *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (UNESCO, 2011), 49 <<http://unesdoc.unesco.org/images/0019/001915/191594e.pdf>> accessed April 2018.

<sup>1144</sup> *ibid* Telegraph Newspaper, (10 December 2008).

<sup>1145</sup> A number of sex and drug education websites had been blocked by Internet filters, leading to a “whitelist” having to be drawn up by January 2014 to prevent charitable websites from being blocked;



Furthermore, Article 10 of the ECHR, also s.10 of the Human Rights Act 1998, confers the right to freedom of expression,<sup>1146</sup> leading one to question how the filters will be able to distinguish between website content which is unlawful and those websites which mention “terrorism” in, for example, a research capacity. These rights are also reflected in Article 15(1) of the Cybercrime Convention which focuses on the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and “*other applicable international human rights instruments*”.<sup>1147</sup> In April 2013, the Special Rapporteur to the United Nations (UN), Frank La Rue, released a report on the freedom of expression and the impact of using surveillance techniques without independent oversight.<sup>1148</sup> La Rue mentions that “[w]ithout explicit laws authorizing [sic] such technologies and techniques, and defining the scope of their use, individuals are not able to foresee – or even know about – their application”<sup>1149</sup> and recommends the use of independent oversight such as the judiciary to monitor States’ use of surveillance.<sup>1150</sup> These observations and recommendations become more concerning in terms of the UK’s proposals on website filtration, as there is a lacuna of information on how ISPs will store information on those opting-in to

---

Ward, M. (BBC News, 31 January 2014) *UK Government tackles wrongly-blocked websites* <<http://www.bbc.co.uk/news/technology-25962555>> accessed November 2016.

<sup>1146</sup> Convention for the Protection of Human Rights and Fundamental Freedoms 1950, Article 10(1).

<sup>1147</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Article 15(1).

<sup>1148</sup> Johnson B. & Arthur, C. (The Guardian, 9 December 2008), *British censor reverses Wikipedia ban* <<https://www.theguardian.com/technology/2008/dec/09/wikipedia-ban-reversed>> accessed November 2016; *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* (A/HRC/23/40), (17 April 2013) <[http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)> accessed November 2016.

<sup>1149</sup> *ibid* La Rue, 13, para. 50.

<sup>1150</sup> *ibid* 22, para. 93; *Yildirim v Turkey* (Application no. 3111/10) HEJUD [2012] ECHR 2074 where the European Court of Human Rights ruled against blanket blocking of websites such as Google Sites. In this case, the Denizli Criminal Court of First Instance upheld an injunction to block Google Sites in order to prevent access to an individual’s website which insulted the First President of Turkey, Mustafa Kemal Atatürk. This was seen as a preventative measure prior to criminal proceedings and used s8(1)(b) of Law No 5651 on regulating Internet publications and combating Internet offences, [56]-[57].

certain websites, as well as whether this information will be used in accordance with freedom of expression principles and existing legislation such as the Terrorism Act 2006.

Function creep and accidental blocking of legal websites are of particular concern as, despite the fact that the filters would potentially cover illegal content such as terrorist financing, they will also cover content considered as ‘harmful’ to under-18s. This could include websites which advocate illegal activity such as underage drinking and pornography, as well as potentially those which advocate strong or extreme political and religious views.<sup>1151</sup> As mentioned above, Article 10 of the ECHR confers the right to freedom of expression,<sup>1152</sup> therefore in this light, the Court of Justice for the European Union (CJEU) set out several important decisions about the compatibility of Internet filtration methods with freedom of expression and the significance of distinguishing between lawful and unlawful content. For instance, the cases of *SABAM v Scarlet*<sup>1153</sup> and *SABAM v Netlog*<sup>1154</sup> both highlight the concerns about methods of Internet filtration which could infringe the rights of freedom of expression and privacy under Articles 10 and 8 ECHR. Although the cases centred on person-to-person file-sharing networks and enforced filtration of copyrighted materials through exceptionally broad injunctions submitted by SABAM,<sup>1155</sup> the CJEU highlighted a key aspect

---

<sup>1151</sup> Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260, 262.

<sup>1152</sup> European Convention on Human Rights, Article 10(1).

<sup>1153</sup> Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011; Reporters without Borders *EU Court says Internet filtering violates freedom of information* (28 November 2011) <<http://en.rsfs.org/european-union-eu-court-says-internet-filtering-28-11-2011.41472.html>> accessed November 2016.

<sup>1154</sup> Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, 16 February 2012; Electronic Frontier Foundation *EU Court of Justice: Social Networks Can't Be Forced to Monitor and Filter to Prevent Copyright Infringement* (17 February 2012) <<https://www.eff.org/deeplinks/2012/02/eu-court-justice-social-networks>> accessed November 2016.

<sup>1155</sup> Directive 2000/31/EC (8 June 2000) Article 45 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), allows for injunctions to be served against ISPs to disable or remove certain content.

of website filtration which must be considered by UK legislators before implementing such a system. Specifically, the Court explained in *Netlog* that “*the injunction could potentially undermine freedom of information, since that [filtration] system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications*”.<sup>1156</sup> As a result, the CJEU is beginning to look into the potential problems filtration systems can cause to lawful websites,<sup>1157</sup> although it is yet to assess cases relating to hosting extremist websites.

The UK is the first EU Member State to use website filtration on this scale, with the European Parliament only going so far as to say that Member States *may* use website filtration to block websites which contain illegal content.<sup>1158</sup> Furthermore, although the E-Commerce Directive,<sup>1159</sup> which allows Member States to require ISPs to remove illegal information,<sup>1160</sup> and the 2006 Revised Action Plan on Terrorism recommended the development of policies to prevent misuse of the Internet by terrorist

---

<sup>1156</sup> *ibid* Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* [52].

<sup>1157</sup> NB. The Treaty of the European Union (“Lisbon Treaty”) has added the Charter of Fundamental Rights to the Community acquis; Beal, K. & Hickman, T. *Beano No More: The EU Charter of Rights After Lisbon* (2011) JR 16(2) 113. Beal and Hickman argue that there will be a convergence in decisions by the ECtHR and the CJEU due to the mirroring of the Charter and ECHR (120-121, paras. 31-33). Furthermore, Beal and Hickman state that the Protocol is essentially only a declaration, and not a general “opt out” of the Charter, 123-125, paras. 40-47.

<sup>1158</sup> E.g. Directive 2011/92/EU (13 December 2011) on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, s. 47.

<sup>1159</sup> Directive 2000/31/EC (8 June 2000) Article 45 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (‘Directive on electronic commerce’).

<sup>1160</sup> E-Commerce Directive, Article 48; *Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment - Addressing the factors contributing to violent radicalisation* COM/2005/0313 (21 September 2005) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0313:FIN:EN:HTML>> accessed November 2016.

websites,<sup>1161</sup> the European Commission stopped short of obliging ISPs to block extremist websites, citing ineffectiveness<sup>1162</sup> and concerns about hampering freedom of expression should a region-wide approach be taken.<sup>1163</sup> Overall, the EU's stance reflects that of the US, leaving it up to ISPs to voluntarily block websites and having no uniform policy on the filtration of websites.<sup>1164</sup> Additionally, the test of freedom of expression and 'harmful' published content was set out in *Handyside v UK*,<sup>1165</sup> when the European Court of Human Rights (ECtHR),<sup>1166</sup> allowed for cultural differences to be taken into account when assessing harmful content against freedom of expression.<sup>1167</sup> However, the Court also noted that freedom of expression *extended* to ideas which could shock or offend.<sup>1168</sup> Despite the UK's Internet filters potentially allowing freedom of expression through an 'opt in' provision, because there is currently no formal legislation and no mention about how the information will be used or stored,

---

<sup>1161</sup> Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260, 263.

<sup>1162</sup> E.g. The European Commission noted that extremist websites could reappear on other hosting ISPs outside the European Union even if they were blocked; *ibid* Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260.

<sup>1163</sup> *ibid* Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260 quoting in the Commission Staff Working Document SEC(2007) 1424 *Accompanying document to the Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism (Impact Assessment)* (6 November 2007), 29 <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2007:1424:FIN:EN:PDF>> accessed November 2016.

<sup>1164</sup> *ibid* Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260.

<sup>1165</sup> *Handyside v UK* App. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737; *ibid* Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260, 262.

NB. The case of *Handyside* related to the publication of a book deemed to be obscene under UK legislation (Obscene Publications Acts 1959 and 1964), as well as accounts of the book published through several national newspapers.

<sup>1166</sup> NB. The European Court of Human Rights is a Council of Europe body, although the European Convention of Human Rights is widely applied across Europe.

<sup>1167</sup> *ibid* *Handyside*, [48].

<sup>1168</sup> *ibid*; Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260, 262.

NB. In *In Vejdeland and others v Sweden* (Application no. 1813/07) [2012] ECHR 242, the European Court recently narrowed the right of freedom of expression to exclude comments which could be construed as "hate speech"; Kiska, R. *Hate Speech: A Comparison between the European Court of Human Rights and the United States Supreme Court* (2012) 25 Regent University Law Review 107.

many Internet users may be reluctant to use the ‘opt in’ feature, potentially dampening their freedom of expression. Consequently, it is difficult to see whether the UK’s far-reaching approach will be compatible with both European policy and be proportionate to the freedom of expression principles currently applied, as well as whether they will comply with the EU guidelines on freedom of expression.<sup>1169</sup> Within those Guidelines, “[t]he right to freedom of expression includes freedom to seek and receive information. It is a key component of democratic governance...”.<sup>1170</sup> Furthermore, the Guidelines have a tripartite test which any interference to freedom of expression must pass before being compatible with both European and international law<sup>1171</sup> – that the interference must be provided by law; that it must pursue one of the purposes set out in Article 19.3 of the International Convention on Civil and Political Rights<sup>1172</sup> and must be proven necessary and as the least restrictive means required and commensurate.<sup>1173</sup> Again, this ties into Article 15(1) of the Convention on Cybercrime, which refers to the Convention on Civil and Political Rights. Finally, the Guidelines state that the EU will “[w]ork against any attempts to block, jam, filter, censor or close down communication networks or any kind of other interference that is in violation of international law.”<sup>1174</sup> The UK’s provisions may work counterintuitively to the EU Guidelines and the Convention on Cybercrime, as there is no clear legal framework to ensure that any blocking of websites by ISPs will not go beyond the initial aims of the Government.

---

<sup>1169</sup> Council of the European Union *EU Human Rights Guidelines on Freedom of Expression Online and Offline* (12 May 2014) <[https://eeas.europa.eu/delegations/documents/eu\\_human\\_rights\\_guidelines\\_on\\_freedom\\_of\\_expression\\_online\\_and\\_offline\\_en.pdf](https://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf)> accessed November 2016.

<sup>1170</sup> *ibid* para.14.

<sup>1171</sup> *ibid* para. 20.

<sup>1172</sup> For example, to protect national security, public order or public health or morals i.e. the principle of legitimacy; *ibid*.

<sup>1173</sup> This would tie in with the aims of proportionality and necessity; *ibid*.

<sup>1174</sup> *ibid* para. 33(d).

Additionally, it is necessary to compare the UK's proposals for website filtration at network level with the US's voluntary arrangements with ISPs to take down illegal websites to assess the appropriateness of this proposal. At the simplest level, the US enshrines the right to freedom of expression in its Constitution,<sup>1175</sup> whereas the UK relies on a mixture of common law and EU legislation to ensure freedom of expression is protected.<sup>1176</sup> Consequently, the UK's stance on freedom of expression is more elastic than the US. As previously mentioned in chapter four, the US case of *Reno v American Civil Liberties Union*<sup>1177</sup> ensured that freedom of expression was extended to website content, putting forward limits to the US government's involvement in regulating 'harmful' Internet content<sup>1178</sup> and highlighting a contrast towards governing the Internet. Furthermore, the US is more cautious than the UK when dealing with unlawful website content, leaving ISPs to voluntarily inform authorities of

---

<sup>1175</sup> The First Amendment of the Constitution of the United States 1787 guarantees freedom of expression <<http://www.usconstitution.net/const.pdf>> accessed November 2016.

<sup>1176</sup> UK citizens have a 'negative' right under the common law, i.e. "*they are free to say anything that is not prohibited...*" Klug, F. Starmer, K. & Keir, S. *The Three Pillars of Liberty: Political Rights and Freedoms in the United Kingdom* (1st Edn. Routledge, 1996), 165; the Human Rights Act 1998 c.42 codifies the European Convention on Human Rights.

<sup>1177</sup> 521 U.S. 844 (1997).

<sup>1178</sup> In *Reno*, the Communications Decency Act 1996, §223 (which criminalised the transmission of 'indecent' material to those under the age of 18 under §233(a), as well as the display of 'patently offensive' content and communications to minors under §233(d)) was deemed to be too vague to uphold the First Amendment. This position was affirmed by the Supreme Court in *Ashcroft v. American Civil Liberties Union* (03-218) 542 U.S. 656 (2004) 322 F.3d 240 when an injunction against the application of CDA's replacement, the Child Online Protection Act of 1998 (Pub. L. 105-277, 112 Stat 2681-728) (15 U.S.C. 6501 et seq.) was upheld because of its vagueness and conflict with the First Amendment. COPA actually provided civil and criminal liabilities for transmitting materials "harmful" to minors (under §231(a)(1),(2) and (3)). The Supreme Court also noted that filters were already available to parents which would not affect their freedom of speech and were less restrictive than the Act. In 2007, the Pennsylvania District Court upheld this decision in *American Civil Liberties Union v Gonzalez* (2007) Civ. NO. 98-5591, holding that the Act was over-broad and vague, also not taking into account the differences in what would be offensive to an eight year old and what would be offensive to a sixteen year old [49], 80; and the Court of Appeals in 2009 upheld this decision in *American Civil Liberties Union et al. v. Mukasey* (3<sup>rd</sup> Cir. 22 July 2008). The Supreme Court ultimately made the Act void by denying the appeal without any comment in *Mukasey v. American Civil Liberties Union et al.* on 21 January 2009; Mears, B. (CNN, 21 January 2009) *Justices refuse to reconsider law restricting Internet porn* <<http://edition.cnn.com/2009/TECH/01/21/supreme.court.reject/>> accessed November 2016.

suspicious activity on the websites they host<sup>1179</sup> and limiting network filtration to very few circumstances.<sup>1180</sup> Therefore, it is difficult to envisage how this mélange of regulation will be reconciled at an international level to ensure an appropriate and effective way of managing websites which solicit donations for terrorist activities.

Because of these differences, it is necessary to make some suggestions to increase both the effectiveness and appropriateness of both the UK's and the US's stance on website monitoring. While voluntary monitoring may seem to be a more constitutionally correct and appropriate way of dealing with extremist websites, without strict guidelines its effectiveness is patchy, with some ISPs likely to be more proactive than others in blocking websites which raise terrorist finances. Leaving it entirely up to ISPs to determine website regulation also creates a conflict in terms of freedom of expression, as some may also have stronger filters than others, thereby accidentally blocking lawful websites. Conversely, while 'opt in' filters may substantially increase the effectiveness of blocking such websites at the ISPs' network source, using such filters is likely to restrict freedom of expression due users' reluctance to opt into unfiltered websites. Consequently, there must be a mid-point between both positions. Instead, by requiring ISPs to monitor website content with a strict set of legislative guidelines to ensure that they can programme blocking technology legally and ethically, this would provide part of the solution to increase effectiveness and balance it

---

<sup>1179</sup> Davis, B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 CommLaw Conspectus 119, 152; Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 Columbia Science and Technology Law Review 5, 11-15.

<sup>1180</sup> E.g. Internet filtration is only enforced in public libraries and schools through the Children's Internet Protection Act of 2000 (Pub.L. 106-554, 114 Stat. 2763) (47 U.S.C. 254 et seq.) - schools and libraries who do not use Internet filtration techniques are denied federal funding discounts through the E-Rate scheme under 47 U.S.C. §254(h)(5)(A)(i)), which has caused some controversy amongst privacy advocates such as the American Civil Liberties Union and the Electronic Frontier Foundation (EFF); Electronic Frontier Foundation *The Cost of Censorship in Libraries: 10 Years Under the Children's Internet Protection Act* (4 September 2013) <<https://www.eff.org/deeplinks/2013/09/cost-censorship-libraries-10-years-under-childrens-internet-protection-act>> accessed November 2016.

with appropriateness. This must also be backed by independent oversight through a judicial tribunal to ensure that neither the ISPs nor governments abuse this power. However, the jurisdictional problems of applying filters or website monitoring on a country-by-country basis would still be apparent if only the UK and the US had standardised Internet regulation. It is also important that regional and international bodies such as the EU and the UN should set the benchmark for website regulation, as they would be able to determine a global standard by which all countries and ISPs could comply.<sup>1181</sup>

Nevertheless, as such an agreement is still likely to be further away than the UK government's proposal for 'opt in' filters; it is worthwhile to make some suggestions to improve the appropriateness of its plans. Firstly, before their application, the UK must provide a clear legislative framework which is narrowly defined to protect freedom of expression and to prevent ISPs from overreaching the aim of the filters. Secondly, if 'opt in' filtration is squarely aimed at one specific section of society (under-18s), then it *must* be limited to material clearly defined as unsuitable for under-18s (such as pornography). If this filtration is also used to prevent terrorist websites from soliciting donations, it must be carried out in line with existing material support and counter-terrorism legislation by balancing public interest with freedom of expression principles, instead of ushering it in because of another reason entirely. Thirdly, the UK Government should provide specific guidelines for ISPs to work with when programming their filters, to prevent lawful websites from being caught by the proposals. These must also include a certain degree of flexibility to allow for the contextualisation of website content. Clearly, it is extremely difficult for ISPs to monitor

---

<sup>1181</sup> NB. This will be set out in more detail in Chapter seven, 7.2., through the analysis of international organisations.



each website individually, therefore, by applying a high percentage of blacklisted terms and images to website content,<sup>1182</sup> this may allow for most lawful websites to remain unaffected while blocking those websites which are specifically used for terrorist support. Finally, there must be independent oversight as to which websites are blacklisted and whether their filtration constitutes an infringement of freedom of expression. Doubtless, such oversight should not be entirely industry-backed nor should it be connected with the UK's government to remain independent. Therefore, it should be connected with the judiciary to be able to provide effective and appropriate supervision. Although these suggestions may not entirely solve the problem of Internet regulation to prevent the proliferation of terrorist websites, they are at least a starting point to evaluate the balance required between the effectiveness and appropriateness of website monitoring and filtration.

### **5.2.2. Electronic Communications**

Since 9/11, the evolution of soliciting donations has meant that electronic communications including email and popular social media fora have become central to raising support and finances.<sup>1183</sup> Therefore, website filtration is likely to become more redundant as terrorists such as ISIL<sup>1184</sup> find other ways of evading jurisdictional censorship. Consequently, after 9/11, the UK also focused upon tracing and monitoring electronic

---

<sup>1182</sup> E.g. If one applies a 90% rate of offensive terms to website content, then ISP filter algorithms would be able to filter those websites which are harmful or illegal without impinging upon those which use the term "terrorism" in a research or journalistic capacity.

<sup>1183</sup> United Nations Office on Drugs and Crime *Use of the Internet for terrorist purposes* (September 2012), 7 para. 14; 35-36

<[http://www.unodc.org/documents/frontpage/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes.pdf](http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf)> accessed November 2016; as an example of raising support via Facebook also see *R v Ahmad (Bilal Zaheer)* [2012] EWCA Crim 959 [2013] 1 Cr. App. R. (S.) 17.

NB. The rise of smartphones and the ability to use mobile banking is also of concern, but will be elaborated upon later in the thesis.

<sup>1184</sup> Also known as Islamic State of Iraq and ash-Sham (ISIS) or Islamic State of Iraq and the Levant (ISIL).

communications as a fundamental aspect of disrupting terrorist financing. As with the US, one of the most controversial aspects of UK legislation, which relates to tracing funds, is contained in its measures against solicitation of donations through private electronic communications. This section is split into three parts. Firstly, an assessment of the appropriateness and effectiveness of intercepting the content of e-mail communications, secondly, appropriateness and effectiveness of overall monitoring of electronic communications, and thirdly, an assessment of the UK's Investigatory Powers Act, which intends to cover both content and non-content of electronic communications.

#### **5.2.2.a. Content of electronic communications**

As explained in chapter three, the UK's surveillance measures are contained within the Regulation of Investigatory Powers Act 2000 (RIPA).<sup>1185</sup> It is necessary to explain that the application of RIPA differs between the collection of 'domestic' or 'internal' email content (sent or received in the UK)<sup>1186</sup> and 'external' email content (or those

---

<sup>1185</sup> NB. As mentioned in chapter three, before RIPA's introduction in 2000, UK authorities relied upon the Interception of Communications Act 1984, c.56 (IOCA), deemed inadequate for computer technologies, due to its focus on postal and public telecommunications system; Jabbour, V. *Interception of Communications - I: Private Rights and Public Policy* (1999) 15 Computer Law and Security Report 6, 390. The restrictions on interception of communications were not applicable to email communications and did not make unauthorised interception an offence; Marès, F., *The Regulation of Investigatory Powers Act 2000: Overview of the case of R v Clifford Stanford (CA (Crim) 211, (1 February 2006) and the Offence of unlawfully intercepting communications on a private system* (2006) 22 Computer Law and Security Report 254, 254; furthermore, the IOCA provisions were deemed incompatible with Article 8(2) of the European Convention on Human Rights, highlighted by the case of *Halford v UK* [1997] ECHR 32, whereby Halford's telephone calls were intercepted on a private telecommunications network. Therefore, the Regulation of Investigatory Powers Act 2000 was introduced primarily to comply with the EU Data Protection Directive (Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and the Privacy in Telecommunications Directive (Directive 97/66/EC (15 December 1997) concerning the processing of personal data and the protection of privacy in the telecommunications sector).

<sup>1186</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 2(4) (b).

sent or received outside the UK).<sup>1187</sup> In this light, domestic communications are afforded far more protection under RIPA than those external communications intercepted by security services.

Regarding internal communications, RIPA provides for the lawful interception of e-mail content through a warrant from the Secretary of State.<sup>1188</sup> This is strictly for the purposes of national security or the detection or prevention of a crime.<sup>1189</sup> However, its effectiveness is somewhat compromised, as telecommunications providers are required to “...provide assistance in relation to interception warrants...”.<sup>1190</sup> This obligation creates complexities in tracing communications which solicit donations. For example, data can be encrypted and identifying users is often problematic.<sup>1191</sup> compromising its effectiveness.<sup>1192</sup> Consequently, some areas of RIPA are open to difficulty when applied.

The problem of applying some areas of RIPA is clear when one assesses the provisions preventing the use of intercept evidence in court. For instance, s.17 specifically excludes intercepted communications gathered under the Act from being used as evidence in legal proceedings,<sup>1193</sup> potentially hampering the Act’s effectiveness in

---

<sup>1187</sup> The meaning of external communications is set out in Regulation of Investigatory Powers Act 2000 c.23, s. 20, which states: “*external communication*” means a communication sent or received outside the British Islands.

<sup>1188</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(3).

<sup>1189</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 5(3)(a)-(d); *R (on the application of ntl Group Ltd) v Ipswich Crown Court* 22 July 2002 [2002] EWHC 1585 (Admin), [2003] Q.B. 131.

<sup>1190</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 11 and s. 12.

<sup>1191</sup> Foundation for Information Policy Research; UK Information Commissioner Study Project: *Privacy and Law Enforcement Paper Number 5* (February 2004), 29 <[www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/conclusion\\_and\\_policy\\_options.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/conclusion_and_policy_options.pdf)> accessed November 2016.

<sup>1192</sup> Although RIPA deals with encryption keys under Title III.

<sup>1193</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 17(1); s.18 outlines the exceptions to using intercept evidence, including its use in closed proceedings under, for example, control order proceedings under the Prevention of Terrorism Act 2005 c.2, s. 18(1)(da).

NB. Intercept evidence prohibitions under RIPA do not apply to interceptions made outside the UK; JUSTICE *Intercept Evidence: Lifting the Ban* (October 2006), 18, para. 41 <<http://www.justice.org.uk/data/files/resources/40/Intercept-Evidence-1-October-2006.pdf>> accessed November 2016; the Report also notes the comments made by Lord Mustill in the case of *R v P* (2001) 2 All ER

anti-terrorism cases and preventing UK law enforcement from using the content of e-mails as evidence of a person's guilt in court. Indeed, the general rule in UK law is to render intercept evidence inadmissible,<sup>1194</sup> in stark contrast to other common law countries such as the US, which allow their prosecutors to use such evidence in criminal proceedings,<sup>1195</sup> highlighting that there are difficulties in fully meeting one of the aims of the 1999 Convention; that of prosecution and punishment of perpetrators of terrorist financing.<sup>1196</sup> Consequently, concerns have been consistently raised about the success of anti-terrorism proceedings due to the lack of intercept evidence; most notably by Lord Lloyd, who stated that there was: *'the difficulty of obtaining evidence on which to charge and convict terrorists, particularly those who plan and direct terrorist activities without taking part in their actual execution.'*<sup>1197</sup> Since 9/11 and the subsequent rise of Internet communications, the question of using intercept evidence has been regularly raised, with the Privy Council advocating a change in the law to

---

58 as follows: *There is no basis for the argument that there is a rule of English public policy which makes this evidence, which is admissible in country 'A', inadmissible in England* – furthermore, the Report explains that RIPA does not preclude foreign courts from using intercept evidence obtained in the UK, [42].

<sup>1194</sup> Telegraph Acts of 1863 Telegraph Act 1863 c. 112 (Regnal. 26 and 27 Vict) and 1868 c. 110 (Regnal. 31 and 32 Vict) prohibited interception and disclosure of telegraph messages by employees (s. 45 of the 1863 Act introduced fines and s. 20 of the 1868 Act introduced a criminal offence); the Birkett Report of 1957 highlighted that it had been “settled policy” of the Home Office *“that, save in the most exceptional cases, information obtained by the interception of communications should be used only for the purposes of detection, and not as evidence in a Court or in any other Inquiry”* (Report of the Committee of Privy Councillors appointed to inquire into the interception of communications Cmnd. 283, para 92 <<http://www.fipr.org/rip/Birkett.htm>> accessed November 2016; *Malone v UK* (1984) 7 EHRR 14, [1984] ECHR 10, [1985] ECHR 5 showed that intercept evidence used in his telephone conversation was obtained contrary to Articles 8 and 13 of the European Convention on Human Rights and resulted in a statutory ban on the use of intercept evidence.

<sup>1195</sup> At a federal level, intercept evidence gathered under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 can be routinely disclosed under testimony in criminal cases; *ibid* 18 U.S.C. §2517(3). Furthermore, §203 of the USA PATRIOT Act of 2001 (Pub. L. 107-56, 115 Stat. 272) enhances existing disclosure rules and applies them to criminal cases involving terrorism.

<sup>1196</sup> Chapter one, 1.4.2.1.

<sup>1197</sup> Lord Lloyd of Berwick *Inquiry into Legislation Against Terrorism* Volume 1 Cm 3420 (HMSO, 1996), para. 7.1.

allow intercept evidence to be used in the case of anti-terrorism control orders.<sup>1198</sup> In particular, the Privy Council explained that there would be a modest increase in successful prosecutions should intercept evidence be used,<sup>1199</sup> and that the Crown Prosecution Service would “[foresee] *savings in court time through more early guilty pleas, and fewer abortive trials*”.<sup>1200</sup> Thus, a review of intercept evidence would enhance the effectiveness of counter-terrorism prosecutions. However, the former Government in 2009 rejected the Privy Council’s findings, stating “[t]hese findings are such that no responsible Government could proceed with implementation on this basis”,<sup>1201</sup> because of cost implications of the legal model proposed<sup>1202</sup> and the requirement for a UK model to be compatible with Article 6 of the ECHR, the right to a fair trial.<sup>1203</sup>

However, the compatibility of intercept evidence with Article 6 of the ECHR is possible, enabling such a measure to be both appropriate and effective. The Privy Council’s proposed legal model along the lines of ‘Public Immunity Interests Plus’ (PII Plus),<sup>1204</sup> failed when tested against Article 6 and the ECtHR decision in *Natunen*<sup>1205</sup> as it placed discretion of evidence submission into the hands of security

---

<sup>1198</sup> Privy Council *Privy Council Review of Intercept as Evidence* Cm 7324 (HMSO, 30 January 2008) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228513/7324.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228513/7324.pdf)> accessed November 2016.

<sup>1199</sup> *ibid* 17, paras. 56, 59; the Review notes the 2006-2007 figures from the Metropolitan Police which states that conviction rates would increase from 88% to 92% should intercept evidence be used.

<sup>1200</sup> *ibid* 15, para. 51.

<sup>1201</sup> Privy Council *Intercept as Evidence: A Report* Cm 7760 (HMSO, 10 December 2009), 4 <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228715/7760.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228715/7760.pdf)> accessed April 2018.

<sup>1202</sup> *ibid* 10, paras. 18-19.

<sup>1203</sup> *ibid* 7-8, paras. 12-14.

<sup>1204</sup> *ibid* 48-49, paras. 206-208. The PII Plus model is found at 44, paras. 191-193. All intercepted evidence would be potentially admissible as evidence and intelligence agencies would decide whether or not to conduct interception of communications to an evidential standard. The agencies would then “retain and record” the intercepted product and transcribe the any sections required by the prosecution while keeping “minimal records” of the rest.

<sup>1205</sup> *Natunen v Finland* (Application no. 21022/04) (2009) 49 EHRR 810. *Natunen* was informed by police that they had recorded 21 telephone conversations relating to drugs trafficking, as well as seven text messages. These had been included in pre-trial proceedings, however, on *Natunen*’s appeal it was found that the police had obtained other recorded telephone conversations which had relevance to the case but had been destroyed. The Court decided that the destruction of the tapes had made it impossi-

agencies. Instead, by allowing intercept evidence to be heard in an open court, and to place all retained information on a suspect at the discretion of the courts, Article 6 would not be compromised. JUSTICE noted, “...*failure to allow intercept evidence in open court has led the government to resort to a variety of exceptional measures*” including control orders and secret inquiries,<sup>1206</sup> which are less appropriate than using intercept evidence. Furthermore, the Privy Council’s proposed models were heavily weighted in favour of surveillance agencies.<sup>1207</sup> Instead, by allowing more judicial control over which pieces of intercepted information should be disclosed in an open court, ECHR rights would not be compromised in cases involving terrorism and more quality convictions could be achieved.

The Privy Council revisited this issue in 2014, providing two new models of intercept evidence,<sup>1208</sup> with the Non-Sensitive Model of intercept evidence found to be compatible with Article 6 ECHR.<sup>1209</sup> Yet, while the Privy Council stated that the “*main potential benefit from the use of intercept material as evidence would be more convictions*”,<sup>1210</sup> it was unable to press forward with intercept evidence due to the potential costs of the exercise.<sup>1211</sup> However, it is essential that the UK Government must

---

ble for Natunen to prove his innocence and, because they had been destroyed at pre-trial stages without the knowledge of Natunen and his defence lawyers and without providing the court with the opportunity of assessing their relevance, that it contravened Article 6 of the ECHR; Reid, J. (former Home Secretary) *Statement to Parliament* HC Deb, c31-32WS (Hansard, 10 December 2009).

<sup>1206</sup> JUSTICE *JUSTICE criticises government delays over intercept evidence* (10 December 2009) <<http://www.justice.org.uk/data/files/resources/62/10dec09-JUSTICE-criticises-government-delays-over-intercept-evidence.pdf>> accessed November 2016.

<sup>1207</sup> *ibid* JUSTICE, Editor’s Note 2.

<sup>1208</sup> These models are (i) The ‘Non-Sensitive’ model. (ii) The Interception Case model; Privy Council *Intercept as Evidence* Cm 8989 (HMSO, 17 December 2014), 16, paras. 43-44 <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/388898/InterceptAsEvidencePrint.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388898/InterceptAsEvidencePrint.pdf)> accessed November 2016.

<sup>1209</sup> *ibid* 17-18, para. 53.

<sup>1210</sup> *ibid* 22, para. 75.

<sup>1211</sup> *ibid* 6, para. 9 – the Privy Council estimated that the costs would range between £4.25bn and £9.25bn over 20 years ‘*depending on assumptions about developing communications technology and usage, and technology costs*’; 6, para. 7.

revisit the issue of intercept as evidence, given the significance and wide-ranging powers of the Investigatory Powers Act,<sup>1212</sup> to make its provisions more appropriate and targeted.

Aside from the ongoing debate about intercept evidence, intercepted domestic communications under RIPA must clearly adhere with ECHR Article 8, or the right to a private life,<sup>1213</sup> as well as the “e-Privacy Directive”,<sup>1214</sup> implemented through domestic legislation. Donohue claims that the original intention behind RIPA was to safeguard privacy from unlawful interception,<sup>1215</sup> but the provisions actually *expanded* the realms in which those with lawful authority may intercept private communications.<sup>1216</sup> For example, in the case of *R (on the application of ntl Group Ltd)*<sup>1217</sup> it was clear that the decision had “*the effect of circumventing the procedures governed*

---

<sup>1212</sup> NB. This will be discussed later. However, JUSTICE, in their written evidence stated at para. 101 that ‘*The failure of this Bill to reconsider the role of intercept material as evidence would represent a missed opportunity for Parliament to bring UK practice into line with the approach in other countries*’ JUSTICE Written Evidence to the Draft Investigatory Powers Bill Joint Committee IPB0148 (HMSO, 17 December 2015)

<[http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#\\_ftn21](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#_ftn21)> accessed November 2016.

<sup>1213</sup> Following Directive 97/66/EC (15 December 1997) concerning the processing of personal data and the protection of privacy in the telecommunications sector, Article 5(1); *Halford v UK* [1997] ECHR 32; Human Rights Act 1998 c.42.

<sup>1214</sup> Directive 2009/136/EC (25 November 2009) amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Directive 2002/58/EC (12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) and Regulation (EC) No 2006/2004. Specifically, the Directive amends the 2002 Directive at Article 1(1) at Article 2. NB. The European Commission introduced Directive 2016/680/EU (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA— this will be discussed on the applicability of the Investigatory Powers Act 2016 c.25 later in the chapter.

<sup>1215</sup> E.g. Donohue, L. K. *Anglo-American Privacy and Surveillance* (2005-6) 96 Journal of Criminal Law and Criminology 1059, 1168; Regulation of Investigatory Powers Act 2000 c.23, s. 1.

<sup>1216</sup> *ibid.*

<sup>1217</sup> *R (on the application of ntl Group Ltd v Ipswich Crown Court* Divisional Court 22 July 2002.

by the RIPA on a sensitive area of law...”,<sup>1218</sup> and consequently “the safeguards of protecting personal privacy from electronic snooping which are embodied in the RIPA [were] to be pushed aside to facilitate the search for criminals...”.<sup>1219</sup> Furthermore, concerns about RIPA and privacy were highlighted when the European Commission launched legal proceedings against the UK for failing to fully implement the e-Privacy and Data Protection Directives.<sup>1220</sup> The UK consequently introduced secondary legislation,<sup>1221</sup> repealing the wording of “reasonable grounds” and limiting surveillance to warrants or direct consent of the individual concerned.<sup>1222</sup> Clearly, a balance is needed between prevention of both terrorist financing and terrorist acts, and the general privacy rights of the majority of Internet users.

Nevertheless, the ECHR provides law enforcement agencies with a loophole to intercept domestic communications in the interests of national security against Article 8(2)’s provision ‘*in accordance with the law*’.<sup>1223</sup> Therefore, the data protection

---

<sup>1218</sup> Lundie, A. *Electronic Commerce – interception of communications – High Court confirms police powers to intercept e-mails* (2003) 9(1) Computer and Telecommunications Law Review N10, 10.

<sup>1219</sup> *ibid* 11; Ferguson, G. & Wadham, J. *Privacy and Surveillance: A review of the Regulation of Investigatory Powers Act 2000* (2003) European Human Rights Law Review 101, 108.

<sup>1220</sup> European Commission *Digital Agenda: Commission refers UK to Court over privacy and personal data protection* (Europa.eu, 30 September 2010) <[http://europa.eu/rapid/press-release\\_IP-10-1215\\_en.htm](http://europa.eu/rapid/press-release_IP-10-1215_en.htm)> accessed April 2018.

NB. The problem was surrounding the issue of consent, whereby the standard was “reasonable grounds”. The case was brought about due to telecoms firms using targeted advertising based on Internet users’ data traffic.

<sup>1221</sup> The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interception) Regulations 2011 SI 2011/1340.

<sup>1222</sup> *ibid.* s. 3 repealing the wording of “reasonable grounds” s. 3(1) of the Regulation of Investigatory Powers Act 2000; Outlaw.com *Revised UK interception of communications laws address EU privacy concerns* (26 January 2012) <<http://www.out-law.com/en/articles/2012/january-/revised-uk-interception-of-communications-laws-address-eu-privacy-concerns/>> accessed November 2016.

<sup>1223</sup> Donohue, L.K. *Anglo-American Privacy and Surveillance* (2005-6) 96 Journal of Criminal Law and Criminology 1059, 1169; Benjamin, V.O. *Interception of Communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Powers Act against the jurisprudence of the European Court of Human Rights* (2007) 6 European Human Rights Law Review 637, 640-641.



and human rights provisions in RIPA do not catch such acts of surveillance.<sup>1224</sup> Moreover, the broad term, *‘in accordance with the law’* has provoked severe criticism from Ferguson and Wadham, who state that there should not just be a legal basis for interception, but that it *“must be adequately accessible and be formulated with sufficient precision to enable citizens to regulate their conduct...”*.<sup>1225</sup> As further outlined, this precision is lacking within RIPA<sup>1226</sup> potentially making the Act open to abuse.

Additionally, with s. 5 RIPA relating to covert surveillance, the Secretary of State must approve a warrant for such surveillance. Therefore, law enforcement authorities do have restrictions when intercepting the content of communications data, addressing the balance between national security and privacy. Furthermore, the only basis for the granting of such warrants is that they are *proportionate* and *necessary*,<sup>1227</sup> bringing the UK into line with Article 8 of the ECHR.<sup>1228</sup> However, some aspects of the allowance of interception are problematic, as *“...the challenge for any new legislation in this field is to provide for effective crime prevention without affecting adversely the rights of the vast majority [of] innocent individuals...”*.<sup>1229</sup> The approval of covert surveillance warrants are criticised by Reid and Ryder who point out that

---

<sup>1224</sup> Jarvie, N. *Control of Cybercrime – is an end to our privacy on the Internet a price worth paying?* Part 2 (2003) 9(2) Computer and Telecommunications Law Review 110, 114.

<sup>1225</sup> *ibid* Ferguson, G. & Wadham, J. *Privacy and Surveillance: A review of the Regulation of Investigatory Powers Act 2000* (2003) European Human Rights Law Review 101, 104.

<sup>1226</sup> *ibid*.

<sup>1227</sup> Akdeniz, Y, Taylor, N. & Walker, C. *Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Review (February) 73-90, 77.

<sup>1228</sup> *ibid*.

<sup>1229</sup> Lloyd, 351.

there is limited judicial intervention,<sup>1230</sup> raising the concern that granting such warrants is not independently appraised.<sup>1231</sup> This is compounded by the fact that the subject of covert surveillance is not informed of the operation, decreasing the opportunity of finding any potential abuse by law enforcement.<sup>1232</sup> Additionally, RIPA allows intelligence services to use surveillance on electronic communications for up to one year in urgent cases and six months in non-urgent cases,<sup>1233</sup> exposing the potential of abuse of private communications.<sup>1234</sup> As a result, the UK's current provisions on covert surveillance are out of balance with key privacy measures, opening up the possibility of abuse.

Furthermore, the use of Interception of Communications Commissioners<sup>1235</sup> in RIPA<sup>1236</sup> has also been the subject of criticism, as they appraise the use of surveillance retrospectively<sup>1237</sup> rather than during the investigation, also viewing surveillance measures randomly.<sup>1238</sup> Nevertheless, the Fourth Chamber of the European Court of Human Rights (ECtHR) found in *Kennedy*<sup>1239</sup> that RIPA and the Commissioner were

---

<sup>1230</sup> Reid, A. S., & Ryder, N., *For Whose Eyes-Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000* (2001) I & CTL, 10 (2), 179-201, 186; Ferguson, G. & Wadham, J. *Privacy and Surveillance: A review of the Regulation of Investigatory Powers Act 2000* (2003) European Human Rights Law Review 101.

<sup>1231</sup> *ibid* Akdeniz et al., 78.

<sup>1232</sup> *ibid* 79.

<sup>1233</sup> "Urgent" cases – those that fall under Regulation of Investigatory Powers Act 2000 c.23, s. 5(3) (s. 9(6)(b) Regulation of Investigatory Powers Act 2000 c.23), e.g. national security or serious crime; "non-urgent" cases – those where renewed surveillance considered to be "necessary" (s. 9(2) and s. 9(6)(c) Regulation of Investigatory Powers Act 2000 c.23); Donohue, L.K. *Anglo-American Privacy and Surveillance* (2005-6) 96 Journal of Criminal Law and Criminology 1059, 1168; Reid, A. S., & Ryder, N., *For Whose Eyes-Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000* (2001) I & CTL, 10 (2), 179-201, 185.

<sup>1234</sup> *ibid* Reid, A.S. & Ryder, N., 187; Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report, Feb, 73, 78.

<sup>1235</sup> These are individuals appointed by the Prime Minister under s. 57(1) Regulation of Investigatory Powers Act 2000 c.23 and review the exercise of powers by the Secretary of State (s. 57(2)) as well as providing support to the Investigatory Powers Tribunal (s. 57(3)). Under s. 57(5), the Commissioner must hold or have held a high judicial office.

<sup>1236</sup> Regulation of Investigatory Powers Act 2000 c.23, Part IV.

<sup>1237</sup> Ferguson, Wadham, 105.

<sup>1238</sup> *ibid*.

<sup>1239</sup> *Kennedy v United Kingdom* (2010) (Application No. 26839/05).

appropriately used and provided strict protection for internal or domestic communications in accordance with the ECHR.<sup>1240</sup> However, the civil liberties organisation JUSTICE criticised this decision on the basis of the “*unquestioning acceptance*” of the Court in the Information Commissioner’s assurances<sup>1241</sup> and the small dip testing used by the Commissioner on warrants issued under RIPA.<sup>1242</sup> Furthermore, should the Commissioner find an inadequate warrant, he is only able to report this to the Prime Minister under s. 58(2) RIPA, leading to concerns about the lack of powers the Commissioner truly has to expose any abuses of power.<sup>1243</sup> Despite the ruling in *Kennedy*, it is concerning that the Commissioner still evaluates only a small proportion of the warrants accepted under RIPA, because such results can only provide an incomplete picture of how these warrants are determined and whether they have been applied appropriately.

Additionally, it was noted that RIPA’s application in *Kennedy* was decided upon a very narrow basis, and that many provisions in RIPA have not been determined as compatible with the ECHR. As Ashworth explained subsequent to the decision, the Court only upheld provisions in RIPA which had judicial oversight in some form (for example, the Investigatory Powers Tribunal) leaving the question of how “designated persons” (such as police officers and security services) use their powers under the Act unanswered.<sup>1244</sup> Furthermore, the Investigatory Powers Tribunal (IPT)<sup>1245</sup> itself has been subject to some criticism, as it was found that only 10 out of 1,120 complaints

---

<sup>1240</sup> *ibid* [169].

<sup>1241</sup> JUSTICE *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), 145, para. 377 <<http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf>> accessed November 2016.

<sup>1242</sup> *ibid* para. 377.

<sup>1243</sup> *ibid* 54, para. 105.

<sup>1244</sup> Ashworth, A. *Case Comment Human rights: Article 8 - right to respect for private life - secret surveillance under powers in Regulation of Investigatory Powers Act 2000* (2010) *Crim. L.R.* 2010, 11, 868, 869-870.

<sup>1245</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 65-70.

had been upheld, leading to a success rate of 0.9% for complainants.<sup>1246</sup> As the report illustrates with regard to counter-terrorism and national security investigations, “*if we were to take the success rate of complaints of the IPT as any kind of an indicator of the quality of surveillance decisions over the past decade, we would have to believe that... surveillance decisions somehow remained miraculously free of error*”.<sup>1247</sup> A reason for such a low rate of upheld complaints was a combination of covert surveillance techniques and a lack of *ex post facto* notification requirements. Therefore, in many cases, individuals simply do not know they have been monitored.<sup>1248</sup> Although it found against some of the tactics security and intelligence agencies used for the first time in 2015,<sup>1249</sup> ultimately, the secretive nature of the Tribunal leads to concerns about discouraging complainants from raising their cases as it would not guarantee an oral hearing, evidence disclosure or judicial review.<sup>1250</sup> While it is clear that RIPA attempts to balance the privacy of most communications with national security in tracing terrorist finances, the extent to which it applies and the lack of judicial intervention creates concern as to how it interacts with privacy law and civil liberties.

The limit of RIPA’s safeguards was revealed in the wake of Edward Snow-

---

<sup>1246</sup> JUSTICE *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011), 136, para. 356 <<http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf>> accessed November 2016. The Report notes that out of these ten cases, six were upheld in 2010 and out of those six, five were lodged individually by members of the same family; Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 121 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018 notes that out of these cases, none were against the security and intelligence agencies.

<sup>1247</sup> *ibid* JUSTICE, 138-139.

<sup>1248</sup> *ibid* JUSTICE, 139, para. 364.

<sup>1249</sup> *Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others* Case Nos IPT/13/77/CH, 13/92/CH, 13/194/C and 13/204/CH [2015] UKIPTrib 13\_77-H, judgments of 5 December 2014 and 6 February 2015.

<sup>1250</sup> *ibid* JUSTICE, para. 366.

den's revelations about the US National Security Agency (NSA) and the UK's intelligence agency, GCHQ.<sup>1251</sup> As mentioned previously, although Chapter I RIPA relates to protections over internal communications carried out in the UK, external communications are open to interception by security services under the Act. Snowden claimed there was a loophole which enabled GCHQ to intercept a wide range of electronic communications through transatlantic fibre-optic cables by using broad certificates relating to external communications under s. 8(4) of RIPA.<sup>1252</sup> Through the TEMPORA system,<sup>1253</sup> which is similar to the NSA's programme PRISM,<sup>1254</sup> GCHQ is potentially able to operate one of the world's largest mass surveillance systems,<sup>1255</sup> simply because the electronic communications have originated outside of the UK. It

---

<sup>1251</sup> Chapter four, 4.3.2. for the background about Edward Snowden, a former National Security Agency operative.

<sup>1252</sup> Snowden revealed that, through using probes attached to transatlantic fibre-optic cables, GCHQ are able to intercept all communications travelling through the UK to Western Europe, including the content of emails, telephone calls, entries on social networking sites and a user's website history. GCHQ then stores this information for 30 days for analysis. Furthermore, GCHQ would also share the contents of the surveillance with the NSA. Snowden showed two documents to The Guardian from GCHQ entitled *Mastering the Internet* and *Global Telecoms Exploitation* which showed the methods of GCHQ's operation TEMPORA; MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. (The Guardian, 21 June 2013) *GCHQ taps fibre-optic cables for secret access to world's communications* <<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>> accessed November 2016.

<sup>1253</sup> Farr, C.B. (Director General of the Office for Security and Counter-Terrorism) *Witness Statement of Charles Blandford Farr on behalf of the Respondents* (Exhibit CF1) in cases IPT/13/92/CH *Privacy International* and (1) *The Secretary of State for Foreign and Commonwealth Affairs* (2) *The Secretary of State for the Home Department* (3) *The Secret Intelligence Service* (4) *The Security Service* (5) *The Government Communications Headquarters* (6) *The Attorney General*; IPT/13/77/H *Liberty* and (1) *The Government Communication Headquarters* (2) *The Secret Intelligence Service* (3) *The Security Service*; IPT/L3/168-173/H (1) *American Civil Liberties Union* (2) *Canadian Civil Liberties Association* (3) *Egyptian Initiative for Personal Rights* (4) *Hungarian Civil Liberties Union* (5) *Irish Council for Civil Liberties* (6) *Legal Resources Centre* and (1) *The Government Communication Headquarters* (2) *The Secret Intelligence Service* (3) *The Security Service*; IPT/13/194/CH *Amnesty International Limited* and (1) *The Security Service* (2) *The Secret Intelligence Service* (3) *The Government Communications Headquarters* (4) *The Secretary of State for Foreign and Commonwealth Affairs*; IPT/13/204/CH *Bytes for All* and (1) *The Secretary of State for Foreign and Commonwealth Affairs* (2) *The Secretary of State for the Home Department* (3) *The Secret Intelligence Service* (4) *The Security Service* (5) *The Government Communications Headquarters* (6) *The Attorney General* (16 May 2014), 16, para. 48 <[https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness\\_st\\_of\\_charles\\_blandford\\_farr.pdf](https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness_st_of_charles_blandford_farr.pdf)> accessed November 2016.

<sup>1254</sup> Chapter four, 4.3.

<sup>1255</sup> *ibid* MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. (The Guardian, 21 June 2013) *GCHQ taps fibre-optic cables for secret access to world's communications* <<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>> accessed November 2016.

was highlighted in alleged UK legal briefings to the US authorities that “[w]e have a light oversight regime compared with the US”.<sup>1256</sup> Therefore, the view of UK security services towards the privacy rights of millions of legitimate Internet users has created widespread concern. For example, both Privacy International and Big Brother Watch began legal action against both GCHQ and the NSA for their surveillance programmes.<sup>1257</sup> Furthermore, although an investigation by the UK Parliament’s Intelligence and Security Committee stated that GCHQ’s TEMPORA programme was conducted in accordance with UK law,<sup>1258</sup> it launched an inquiry on legal framework surrounding the interception of communications.<sup>1259</sup> The All Party Parliamentary Group on Drones were provided with expert legal advice on mass surveillance by Jemima Stratford QC, who advised that such surveillance could be conducted using gaps in

---

<sup>1256</sup> *ibid.*

<sup>1257</sup> Hopkins, N. (The Guardian, 8 July 2013) *NSA and GCHQ spy programmes face legal challenge* <<http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge>> accessed November 2016; Privacy International *Statement of Grounds to the Investigatory Powers Tribunal* (9 July 2013) <[https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy\\_international\\_ipt\\_grounds.pdf](https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_ipt_grounds.pdf)> accessed November 2016.

With regard to Big Brother Watch, it brought legal action with other agencies before the European Court of Human Rights for violations of Article 8 ECHR in September 2013; (1) *Big Brother Watch* (2) *Open Rights Group* (3) *English PEN* (4) *Dr Constanze Kurz v United Kingdom* (Application No. 58170/13) [2014] ECHR 93. The UK Government was ordered to provide a submission to the Court; Hopkins, N. (The Guardian, 24 January 2014) *Justify GCHQ mass surveillance, European court tells ministers* <<http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights>> accessed November 2016.

<sup>1258</sup> Intelligence and Security Committee/Rt. Hon. Sir Malcolm Rifkind MP (Chairman) *Statement on GCHQ’s Alleged Interception of Communications under the US PRISM Programme* (17 July 2013) <<http://isc.independent.gov.uk/news-archive>> accessed November 2016; it explained that, after reviewing intelligence reports, there was no evidence that the intelligence services had circumvented UK law, namely Regulation of Investigatory Powers Act 2000 c.23 and the Intelligence Services Act 1994 c.13 <<http://isc.independent.gov.uk/news-archive>> accessed November 2016 but the document itself is available through <[https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717\\_ISC\\_statement\\_GCHQ.pdf?attachauth=ANoY7cpLxxOKh-nyX1hxSFjznfDNoE3oLFdOclZ-svLhbMjvZLZL\\_JQDldyVkNI0a-zWqcsQpHaAx8dQkl-Roo1Lwl1PC71gf5cYKo70g-AraGwDVZzIDEGpkPxRHXOT4Ivi-pM8CDr\\_XXCcy2H0YiDqYfg7AQugLHoZJgz9YtF6\\_Y6OvokW2yO79n1gIxQYgAIGJN5pT-aUlwpH5QDU48u2h7Dbzx5KcCDQ2OgUP3wJlkjEUwcBGNE%3D&attredirects=0](https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf?attachauth=ANoY7cpLxxOKh-nyX1hxSFjznfDNoE3oLFdOclZ-svLhbMjvZLZL_JQDldyVkNI0a-zWqcsQpHaAx8dQkl-Roo1Lwl1PC71gf5cYKo70g-AraGwDVZzIDEGpkPxRHXOT4Ivi-pM8CDr_XXCcy2H0YiDqYfg7AQugLHoZJgz9YtF6_Y6OvokW2yO79n1gIxQYgAIGJN5pT-aUlwpH5QDU48u2h7Dbzx5KcCDQ2OgUP3wJlkjEUwcBGNE%3D&attredirects=0)> accessed November 2016; Rt Hon William Hague MP, *Foreign Secretary responds to Intelligence and Security Committee* <<https://www.gov.uk/government/news/foreign-secretary-responds-to-intelligence-and-security-committee-statement-on-gchq>> accessed November 2016.

<sup>1259</sup> Intelligence and Security Committee *Privacy and Security Inquiry - Call for Evidence* (11 December 2013) <<http://isc.independent.gov.uk/news-archive/11december2013>> accessed November 2016.

legislation, which affords “*too wide a discretion to the Secretary of State*”,<sup>1260</sup> providing “*almost no meaningful restraint on the exercise of executive discretion in respect of external communications*”<sup>1261</sup> and are a “*disproportionate interference*” with rights set out under Article 8 ECHR.<sup>1262</sup> This was a position later backed up by the Investigatory Powers Tribunal in *Liberty and others*,<sup>1263</sup> whereby it found that the NSA and GCHQ’s surveillance techniques had contravened Articles 8 and 10 of the ECHR. This has since been rectified by the security services.<sup>1264</sup>

Critically, the advice highlights the differences between warrants relating to domestic and external communications, showing that the certificates used to access external communications could be based on broad keywords or affect a large number of individuals, rather than using specific terms or individuals.<sup>1265</sup> Thus, allowing security services to intercept mass communications originating from overseas without the same legal oversight as those between two individuals based in the UK. The advice also surmises that, if the transatlantic cable interceptions included in GCHQ’s TEMPORA programme included UK domestic communications routed through the US,

---

<sup>1260</sup> Stratford, J., Johnston, T. Brick Court Chambers, (22 January 2014) *In the matter of surveillance: Advice*, 14, para. 45 <[http://www.brickcourt.co.uk/news-attachments/APPG\\_Final\\_\(2\).pdf](http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf)> accessed June 2018; All Party Parliamentary Group on Drones *Jemima Stratford QC’s Advice* (29 January 2014) <<http://appgdrones.org.uk/jemima-stratford-qcs-advice/>> accessed June 2018.

NB. Stratford and Johnston also wrote an article on this issue, explaining that RIPA’s measures with regard to external communications were “*very probably unlawful*”; Stratford, J. & Johnston, T. *The Snowden “revelations”: is GCHQ breaking the law?* E.H.R.L.R. 2014, 2 129, 135.

<sup>1261</sup> *ibid.*

<sup>1262</sup> *ibid* Stratford & Johnston, Brick Court Chambers (22 January 2014) *In the matter of surveillance: Advice*, 3, para. 7(a) <[http://www.brickcourt.co.uk/news-attachments/APPG\\_Final\\_\(2\).pdf](http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf)> accessed June 2018.

<sup>1263</sup> *Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others* Case Nos IPT/13/77/CH, 13/92/CH, 13/194/C and 13/204/CH [2015] UKIPTrib 13\_77-H, judgments of 5 December 2014 and 6 February 2015.

<sup>1264</sup> *ibid.*

<sup>1265</sup> *ibid* Stratford & Johnston, *In the matter of surveillance: Advice*, 2, para. 14; at para. 15, it notes: *In short ‘external’ warrants allow for interception of bulk or mass data, ‘internal’ warrants do not.*

then this would breach RIPA protections.<sup>1266</sup> Consequently, it was very clear that the oversight and powers contained within RIPA needed to be reviewed extensively in order to make its use appropriate when balancing interception of suspected terrorist telecommunications with privacy rights of the majority of Internet users. Such a review of surveillance legislation eventually happened in 2015, when David Anderson QC the Independent Reviewer of Terrorism Legislation published *A Question of Trust*, which advocated<sup>1267</sup> a wholesale reworking of surveillance legislation including RIPA, so that tougher safeguards were implemented to protect privacy, which will be discussed in depth during the next section.<sup>1268</sup>

#### **5.2.2.b. Non-content of electronic communications**

Snowden's revelations also included the sheer amount of the non-content or "metadata" of electronic communications, such as names and IP addresses, collected by GCHQ and private communications providers, although these centred on external, or non-domestic communications. However, security services and law enforcement authorities can legally access the non-content of domestic communications under s22

---

<sup>1266</sup> *ibid* 8-9, paras. 19-25; C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971 which held that to place information on a website "*did not constitute transferring that data to third countries outside the EU, even if the server hosting the website was in a third country*", [22]. NB. In April 2014, the Interception of Communications Commissioner, Sir Anthony May, dismissed allegations that GCHQ circumvented UK legislation or conducted mass surveillance after an investigation into Snowden's revelations; Interception of Communications Commissioner's Office *2013 Annual Report of the Interception of Communications Commissioner* <<http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf>> accessed November 2016; Whitehead, T. (The Telegraph, 8 April 2014) *GCHQ given all clear over Edward Snowden allegations by watchdog* <<http://www.telegraph.co.uk/news/uknews/law-and-order/10752205/GCHQ-given-all-clear-over-Edward-Snowden-allegations-by-watchdog.html>> accessed November 2016.

<sup>1267</sup> Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015) <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018.

<sup>1268</sup> *ibid*.



of RIPA,<sup>1269</sup> and intelligence services can collect non-content data in bulk, in the interests of national security.<sup>1270</sup> This is defined by Whitley and Hosein as “...*storing all of this data, for all communications and transactions, for a period of time (and in particular, for longer than it would be kept for purely billing and engineering purposes) ...*”.<sup>1271</sup> This includes time, date and identification of the sender and recipient of this data, the retention of communications data has raised various arguments in favour of, and against, its use. After 9/11, it was argued by law enforcement that “...*legislation was required to ensure that the data they wished to access was not deleted by CSPs [Communication Service Providers] before such access could be granted...*”<sup>1272</sup> which would make their investigations into criminal activity less effective. Consequently, it is clear that law enforcement agencies required the retention of data for law enforcement purposes, especially anti-terrorism, after 9/11.

Currently, ISPs can avoid civil liability if they lawfully obtain and disclose communications data under s. 21 of RIPA, increasing the effectiveness of detecting communications relating to terrorist financing. Essentially, access to metadata has been simplified through the use of RIPA, making it an effective tool to trace terrorist communications. Additionally, the introduction of Directive 2006/24/EC on the retention of data went further, creating an obligation for ISPs<sup>1273</sup> to retain and archive

---

<sup>1269</sup> Regulation of Investigatory Powers Act 2000 c.23, s. 22 allows certified persons under the Act to obtain traffic or communications data if it is necessary under a number of grounds to do so, for example, in cases of national security under s. 22(2)(a).

<sup>1270</sup> Telecommunications Act 1984, s. 94 as amended by the Communications Act 2003 c.21 – these do not require judicial warrants, just approval from the Home Secretary (s. 94(1) Telecommunications Act 1984).

<sup>1271</sup> Whitley, E.A. & Hosein I. *Policy Discourse and data retention: the technology politics of surveillance in the United Kingdom* (2005) 29 Telecommunications Policy 357, 360.

<sup>1272</sup> *ibid* 327.

<sup>1273</sup> Directive 2006/24/EC (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, Article 3(1).

data for interception purposes for a period of 12 months,<sup>1274</sup> creating a legal framework for law enforcement to access communications data. The UK adopted the Directive in 2009,<sup>1275</sup> covering outside communications and potentially increasing effectiveness by adopting a region-wide and uniform legal requirement when retaining and accessing data for national security purposes. The Directive required ISPs to retain data relating to user IDs, names and addresses of the registered user or subscriber of the Internet Protocol (IP) address, as well as the destination number or IP address of an email or Internet communication,<sup>1276</sup> for a period of 6 months to two years,<sup>1277</sup> heightening the ability of government agencies to gather evidence against potential terrorist communications. However, this effectiveness may now be compromised, as the CJEU declared the Directive to be invalid, after legal challenges by Austria and Ireland<sup>1278</sup> to the Directive's validity, with reference to two fundamental rights of the EU Charter,<sup>1279</sup> the right to a private life and the right to protection of personal data under Articles 7 and 8. Here, the CJEU identified that the data retained, including date, time and frequency of the communications, as well as the identity of the user and

---

<sup>1274</sup> Directive 2006/24/EC (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, Article 5.

<sup>1275</sup> NB. The UK actually delayed implementing the Data Retention Directive under Article 15(3) until March 2009; Goodall, J., *United Kingdom: Data Retention Directive* (2007) Data Protection Law and Policy, April 2007.

<sup>1276</sup> Directive 2006/24/EC (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, Article 5(2).

<sup>1277</sup> Directive 2006/24/EC (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, Article 6.

<sup>1278</sup> Joined cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others. Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221.

<sup>1279</sup> Also known as the Charter of Fundamental Rights of the European Union 2000/C 364/01 (2010/C 83/02); introduced in 2000 and made legally binding after the passage of the Lisbon Treaty <<http://ec.europa.eu/justice/fundamental-rights/charter/>> accessed November 2016.

the place they communicate from, taken together provide a precise information on the private life of an individual and, because of the increasing importance of Internet communications, the Directive constituted “*an interference with the fundamental rights of practically the entire European population*”.<sup>1280</sup> Additionally, the CJEU found that the Directive did not contain clear limits to access by national authorities or authorised persons, as well as a lack of intervention by national courts to determine whether such access is appropriate.<sup>1281</sup> Weighed up against the necessity of national security, the Directive’s provisions on data retention and information about an individual, the CJEU decided, was not proportionate to the protections afforded in Articles 7 and 8 of the EU Charter.

This is a significant decision with regard to the UK’s position on data retention as, although the UK opted out of certain crime and justice provisions of the Lisbon Treaty,<sup>1282</sup> it may still have far-reaching consequences for the application of future legislation on data collection and retention, such as the Investigatory Powers Act.<sup>1283</sup> Furthermore, the UK is legally bound by the Charter, potentially limiting the scope of its data retention and access policies. For instance, the CJEU held in *N.S. v Home*

---

<sup>1280</sup> C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others. Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221, [56].

<sup>1281</sup> *ibid* [60]-[62].

<sup>1282</sup> The UK opted out of 100 of 135 crime and justice provisions under Protocol 36 of the Lisbon Treaty on 1 December 2014. 11 out of the remaining 35 provisions are outlined in the Criminal Justice and Data Protection (Protocol 36) Regulations 2014 SI 2014/3141, including applying the European Arrest Warrant (Chapter 2) and the freezing of assets and property relating to the proceeds of crime (Chapter 2). The Explanatory Memorandum to the Regulations states that the other provisions will require further transposition into UK law ([4.4.], 4, Explanatory Memorandum).

<sup>1283</sup> The Act was first introduced in Autumn 2015; Secretary of State for the Home Department, *Oral Statement to Parliament on the Publication of the Anderson Report* (11 June 2015) <<https://www.gov.uk/government/speeches/home-secretary-on-publication-of-the-anderson-report>> accessed November 2016.

Secretary<sup>1284</sup> that Article 51(1)<sup>1285</sup> of the Charter and Protocol 30 of the Lisbon Treaty “does not intend to exempt... the United Kingdom from the obligation to comply with the provisions of the Charter or to prevent a court of one of those Member States from ensuring compliance with those provisions”.<sup>1286</sup> The House of Commons European Scrutiny Committee confirmed this position,<sup>1287</sup> highlighting that the Charter is applicable when a Member State acts within the scope of EU law, as shown in *Fransson*.<sup>1288</sup> As both data retention and data protection are potentially within the scope of EU law,<sup>1289</sup> the UK may be required to have regard to the Charter and the CJEU’s decision when implementing subsequent legislation to access and retain metadata, potentially

---

<sup>1284</sup> Cases C-411/10 and C-493/10, *N.S. v Home Secretary and M.E. v. Refugee Applications Commissioner* [2011] EUECJ C-411/10 (21 December 2011).

<sup>1285</sup> Lisbon Treaty, Article 51(1).

<sup>1286</sup> *ibid* Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221, [120].

<sup>1287</sup> European Scrutiny Committee *The EU Charter of Fundamental Rights in the UK: a state of confusion* (HMSO, Forty Third Report of Session 2013-14) <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmeuleg/979/979.pdf>> accessed November 2016.

<sup>1288</sup> C-617/10 *Åklagaren v Hans Åkerberg Fransson* (2013) – although this was a case about taxation, the CJEU in its judgement stated at paragraph 21 that “Since the fundamental rights guaranteed by the Charter must therefore be complied with where national legislation falls within the scope of European Union law, situations cannot exist which are covered in that way by European Union law without those fundamental rights being applicable. The applicability of European Union law entails applicability of the fundamental rights guaranteed by the Charter”, [21]; highlights added by the author in respect of proposed UK legislation on data retention.

<sup>1289</sup> E.g. The Data Retention Directive (Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and The Directive on Privacy and Electronic Communications (Directive 2002/58/EC (12 July 2002) concerning the processing of personal data and the protection of privacy in the electronic communications sector).

hampering their effectiveness.<sup>1290</sup> Furthermore, the Convention on Cybercrime specifically refers to data preservation, rather than data retention,<sup>1291</sup> putting the UK in conflict with its minimum standards. As Vatis outlines, there is an inherent difference between the data preservation requirements of the Convention and that of data retention.<sup>1292</sup> Significantly, he notes that “*amendments were made to clarify that the Convention did not mandate data retention or the use of specific interception technologies, to make clear that states would not criminalise the development or use of network security testing tools, and to limit the vicarious liability of corporations*”.<sup>1293</sup> By comparison, Article 16 of the Convention specifically states that legislative measures should be applied “*oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days*”.<sup>1294</sup> As a result, it is questionable whether data retention itself is appropriate.

Yet, the Data Retention and Investigatory Powers Act 2014 (DRIPA) seeks to temporarily fill the gap the CJEU’s decision has made, to continue capturing information on potential terrorist suspects and avert terrorist attacks. For instance, the Act ensures that telecommunications data is retained for a period “*not exceed[ing] 12*

---

<sup>1290</sup> NB. There have been no test cases as such, however, the Supreme Court’s view only two weeks later in the case of *R (on the application of HS2 Action Alliance Limited) (Appellant) v The Secretary of State for Transport and another (Respondents)*, [2014] UKSC 3 was that EU law should not be interpreted as: “...either to require UK courts to adjudicate on, with the corollary of being able to strike down, national parliamentary procedures; or to require the abrogation of fundamental constitutional principles, in the UK, notwithstanding the European Communities Act 1972.” It remains to be seen whether UK courts can prevent CJEU intervention once the Investigatory Powers Act is in force.

<sup>1291</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Articles 16 and 17.

<sup>1292</sup> Vatis, M. A. *The Council of Europe Convention on Cybercrime, 2010*, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy <<http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf>> accessed April 2018.

<sup>1293</sup> *ibid* 218 (fn. 92); European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Article 16(1).

<sup>1294</sup> *ibid* 212 (fn41).

months”,<sup>1295</sup> far exceeding the requirements of the Cybercrime Convention, as outlined above, but in line with the original implementing Data Retention (EC Directive) Regulations 2009.<sup>1296</sup> This is specifically to retain some powers of law enforcement to effectively find terrorist communications. Given the heightened security concerns surrounding the terrorist group ISIL and their use of social media to spread their message, raise finances and to plan future terror attacks,<sup>1297</sup> the decision to enable law enforcement to access communications data is essential. The Act sunsets in December 2016,<sup>1298</sup> therefore the UK Government must act quickly in order to cover any gaps left by the *Digital Rights Ireland* decision. However, such action must have regard to both the Convention on Cybercrime, and the High Court’s judgement in *R (on the application of David Davis MP et al) v The Secretary of State for the Home Department*,<sup>1299</sup> which may act as a presage for the courts’ views on any future legislation surrounding access to data retention and, as will be discussed later with regard to the Home Secretary’s appeal, the CJEU’s stance on the retention of general communications data. Here, the High Court ruled that s. 1 of the Act on retention notices did not lay down clear and precise rules to restrict the access and use of communications data to strictly defined serious offences.<sup>1300</sup> Furthermore, the Court found that access to such retained data under the retention notice was not subject to or made dependent upon review by either a court or an independent administrative body. Such bodies,

---

<sup>1295</sup> Data Retention and Investigatory Powers Act 2014 c.27, s. 1(5).

<sup>1296</sup> The Data Retention (EC Directive) Regulations 2009 SI 2009/859, s. 5.

<sup>1297</sup> Home Office *CONTEST, the United Kingdom’s strategy for countering terrorism: annual report for 2014* (23 March 2015) <<https://www.gov.uk/government/publications/contest-uk-strategy-for-countering-terrorism-annual-report-for-2014>> accessed June 2018; David Anderson QC *A Question of Trust* (HMSO, June 2015), [3.16], 43 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018..

<sup>1298</sup> Data Retention and Investigatory Powers Act 2014 c.27, s. 8(3).

<sup>1299</sup> *R (on the application of David Davis MP, Tom Watson MP, Peter Brice, Geoffrey Lewis) v The Secretary of State for the Home Department and Open Rights Group, Privacy International, The Law Society of England and Wales* [2015] EWHC 2092 (Admin).

<sup>1300</sup> *ibid.*

the Court argued, would be able to define what is ‘strictly necessary’ for attaining the objective of the retention notice.<sup>1301</sup> Additionally, David Anderson QC heavily criticised RIPA as “*incomprehensible to all but a tiny band of initiates*”<sup>1302</sup> due to being “*patched up so many times*”.<sup>1303</sup> He recommended that a “*comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive power that may be necessary for public authorities to use...* ”.<sup>1304</sup> On the issue of data retention, Anderson suggested that, while gathering retained data would be useful for gathering information, a rigorous assessment needed to be made on the lawfulness, effectiveness and intrusiveness, as well as cost implications of a requirement to retain such data.<sup>1305</sup> Specifically, Anderson also recommended that the judgement of *Digital Rights Ireland* should be adhered to, in particular, a limitation of the data accessed, reasonable retention periods and destruction of data when the retention period ends.<sup>1306</sup> Consequently, both Anderson and *Davis* highlight the desirability for judicial oversight in surveillance legislation, in order to make, for example, retention notices, appropriate and compatible with the decision in *Digital Rights Ireland* and Articles 7 and 8 of the EU Charter.

### 5.2.3. **The Investigatory Powers Act**<sup>1307</sup>

---

<sup>1301</sup> *ibid.*

<sup>1302</sup> Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 8, para. 35 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018..

<sup>1303</sup> *ibid.*

<sup>1304</sup> *ibid* Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 4, para. 10 Recommendations 1-9 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018.

<sup>1305</sup> *ibid* 5, para. 13(b); Recommendations 15-18.

<sup>1306</sup> *ibid* Recommendation 16.

<sup>1307</sup> At the time of submitting this thesis (1 December 2016), while the Act received Royal Assent (29 November 2016), many of its provisions had not yet been brought into force.

The UK Government's response to both *Digital Rights Ireland* and the Anderson Review, the Investigatory Powers Act, was introduced in March 2016.<sup>1308</sup> The Act itself has several purposes: to codify existing powers to law enforcement and intelligence agencies to obtain data communications, to introduce a 'double lock' for an interception warrant so that they must be approved by a judge as well as the introduction of an Investigatory Powers Commissioner and judicial commissioners, and finally making provision for the retention of internet connection records, '*for law enforcement to identify the communications service to which a device has been connected*'.<sup>1309</sup> Potentially, the Act provides a balance between the need for an effective strategy on future interception of communications and the requirements of necessity and proportionality.<sup>1310</sup> For the purposes of this thesis, the Act has two main strands, to increase effectiveness and to cover the gaps left by the decision in *Digital Rights Ireland*, Snowden's revelations and replacing some of the "*sometimes opaquely*"<sup>1311</sup> defined powers under RIPA to intercept communications.

First, the Act requires telecommunications operators under a retention notice from the Home Secretary "*to retain relevant communications data if the Secretary of*

---

<sup>1308</sup> NB. It was reintroduced after the Joint Committee on the Investigatory Powers Bill *Report of Session 2015-16* HL Paper 93/HC 651 (HMSO, 11 February 2016) <<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm>> accessed November 2016.

<sup>1309</sup> Home Office *Investigatory Powers Bill* (1 March 2016) <[www.gov.uk/government/collections/investigatory-powers-bill](http://www.gov.uk/government/collections/investigatory-powers-bill)> accessed November 2016.

NB. This quote relates directly to Internet Connection Records, which will be discussed below.

<sup>1310</sup> For example, as noted in *A Question of Trust*, wireless technology which creates shared IP addresses, smart phones and proxy servers all pose a significant problem for intelligence agencies to identify data communications from one specific subject (Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 53-54 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018).

<sup>1311</sup> Anderson D. *Legislation Report of the Bulk Powers Review* Cmd 9326 (HMSO, August 2016), 7 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>> accessed June 2018.



*State considers that the requirement is necessary and proportionate*”<sup>1312</sup> and the retention of data is limited to a period of up to twelve months,<sup>1313</sup> reflecting the temporary measures outlined in DRIPA. Access to retained communications data enables UK intelligence and law enforcement authorities to investigate and gather information about potential terrorist acts, increasing their effectiveness, but reducing their compatibility with the Convention on Cybercrime. The Act also goes further than DRIPA, by providing a new power to acquire retained Internet Connection Records,<sup>1314</sup> something that neither any EU Member State nor even the US has in force.<sup>1315</sup> This power would enable law enforcement agencies to access the Internet connections from, for example, a device such as a smartphone which accessed a certain social media website.<sup>1316</sup> This would allow law enforcement agencies to attribute an illegal activity on the Internet to an individual, increasing the likelihood of capturing an illegal act online.<sup>1317</sup> Consequently, this allows law enforcement to identify the sender of a social message on, for example, raising funds for a proscribed terrorist organisation, which are currently not covered by data communications requests.<sup>1318</sup> As online messaging becomes more readily used, 19 billion online messages were sent in 2012, compared with 17.6 billion text messages, and ISIL have been prolific in using online

---

<sup>1312</sup> Investigatory Powers Act 2016 c.25 Part 4, s. 87(1)(a) – proportionality and necessity is defined in s. 53(1) and s. 20 of the Act, e.g. national security (20(2)(a)), and detection of crime and prevention of disorder (20(2)(b))) .

<sup>1313</sup> Investigatory Powers Act c.25 Part 4, s. 87 on retention notices.

<sup>1314</sup> Investigatory Powers Act c.25 Part 4, s. 87(11) and s. 62.

<sup>1315</sup> *ibid* Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 256 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018.

<sup>1316</sup> Home Office Factsheet *Investigatory Powers Bill: Internet Connection Records* (30 October 2015) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530556/Internet\\_Connection\\_Records\\_factsheet.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf)> accessed November 2016.

<sup>1317</sup> *ibid*.

<sup>1318</sup> *ibid*.

messaging services to recruit and raise funds,<sup>1319</sup> this attempts to cover lacunae left by evolving technology, which is key in intercepting communications between individuals and terrorist organisations. However, as Liberty outlined, the Internet Service Providers Association outlined a major flaw in the collection of Internet Connection Records as they “*would not accurately show when communications services have been used, and therefore would not be helpful for informing an accurate time frame for further communications data requests*”.<sup>1320</sup> This is because communications software can stay connected in the background, whether in use or not, which means, for example, a smartphone, can be connected to a network for days, weeks or months.<sup>1321</sup> The use of Virtual Private Networks (VPNs) would also counteract Internet Connection Records, as the Internet Service Provider would only be able to see the data traffic sent to the VPN provider, without any information on the true destination or the contents.<sup>1322</sup> This problem is compounded when using an overseas provider, as there is no jurisdiction for UK law enforcement authorities to automatically receive this

---

<sup>1319</sup> For example, at its height during the capture of Mosul in 2014, ISIL sent out 40,000 tweets in a single day; Irshaid, F. (BBC News 19 June 2014) *How Isis is spreading its message online* <<http://www.bbc.co.uk/news/world-middle-east-27912569>> accessed November 2016; Neumann, P. R. *Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s* (ICSR 26 January 2015) <<http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>> accessed November 2016; Berger, J.M. *Tailored Online Interventions: The Islamic State's Recruitment Strategy* (Combating Terrorism Center, 23 October 2015) <[https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy](https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy;)> accessed November 2016; Ali Shukri Amin, a United States teenager, was convicted in 2015 for soliciting donations for ISIL through Twitter and Bitcoin; *United States v. Ali Shukri Amin* Criminal No: 1:15-cr-164 in the Eastern District of Virginia, Alexandria Division.

<sup>1320</sup> Liberty *Liberty's written evidence on the Investigatory Powers Bill* (March 2016), 28, para. 60 <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.

<sup>1321</sup> *ibid.*

<sup>1322</sup> Lloyd, C. *Written evidence submitted to the Public Bills Committee* IPB 35 (HMSO, 24 March 2016) <<http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB35.htm>> accessed November 2016.

data.<sup>1323</sup> Finally, the use of the TOR network by criminal organisations is well-documented,<sup>1324</sup> and due to the ‘onion’ router, communications data is routed several times, “so that no one other than the original user knows the true source and destination addresses”.<sup>1325</sup> This means that the only information the Internet Service Provider can see is the user connecting to a TOR browser on the Dark Web.<sup>1326</sup> Consequently, it is difficult to see whether the Act’s proposals will be effective enough to detect terrorist communications thoroughly, especially with the evolution of technology to encrypt and evade law enforcement.

Second, the Act permits security services to access and collect “bulk” data communications – which, despite Snowden’s revelations, is still accepted as a necessary tool in identifying, disrupting and investigating terrorist communications.<sup>1327</sup> For example, as Anderson outlined,<sup>1328</sup> bulk collection of overseas data communications and access to bulk personal datasets<sup>1329</sup> were key to quickly identifying the perpetrators of the Paris and Brussels attacks in 2015,<sup>1330</sup> as well as those who posed a threat

---

<sup>1323</sup> *ibid.*

<sup>1324</sup> For example, Silk Road is the most famous example of using the TOR network on the Dark Web; *United States of America v. Ross William Ulbricht a/k/a ‘Dread Pirate Roberts’, a/k/a ‘DPR’, a/k/a ‘Silk Road’* 14-cr-68 (October 30, 2014); a recent study in 2016 also showed that 57% of the sites used on TOR were for illicit activity, Moore, D. & Rid, T. *Cryptopolitik and the Darknet, Survival* (2016) Vol. 58 Iss. 1

<<http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>> accessed November 2016.

<sup>1325</sup> *ibid* Lloyd, C., *Written Evidence*.

<sup>1326</sup> *ibid.*

<sup>1327</sup> *Szabó and Vissy v Hungary* (Application no. 37138/14) (Court (Fourth Section)), [2016] ECHR 579, [68].

NB. The Court found that the Hungarian law was in breach of Article 8 of the ECHR, and potentially outlawing mass surveillance – although the judgement itself is ambiguous.

<sup>1328</sup> Anderson D. *Legislation Report of the Bulk Powers Review* Cmd 9326 (HMSO, August 2016) <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>> accessed June 2018.

<sup>1329</sup> NB. Bulk Personal Datasets are files on large groups of people which contain information, such as appearances on the Electoral Roll and travel information; Home Office *Bulk Personal Data Factsheet for the Investigatory Powers Bill* (4 March 2016) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530548/BPD\\_Factsheet.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530548/BPD_Factsheet.pdf)> accessed November 2016.

<sup>1330</sup> *ibid* Anderson, D., 114, 193 (A11/5 Case Study).

to the UK in the wake of these attacks.<sup>1331</sup> Furthermore, the short timescales between identifying and disrupting a potential terrorist act through bulk data collection are clear, with MI5 outlining that it took just two weeks between identifying an individual set to carry out numerous attacks in European cities via bulk communications acquisition, and his eventual capture through provision of information and liaising with European security services.<sup>1332</sup> As a result, it is clear that the Act aims to continue the effectiveness of current powers on acquiring and intercepting bulk data.

In order to bring it into line with *Digital Rights Ireland* and the appropriateness of such measures, the Act seeks to create some parity with this decision. According to Anderson, it “*stands not only for transparency but for the introduction of new safeguards*”<sup>1333</sup> including judicial approval for warrants and creating the Investigatory Powers Commissioner, who would oversee a single new supervisory body.<sup>1334</sup> Therefore, that interception warrants under the Act would have to be analysed and agreed with a Judicial Commissioner, rather than a single ‘rubber stamp’ exercise by the Home Secretary, as happened under RIPA. Furthermore, the introduction of an Investigatory Powers Commissioner, who would oversee the activity of the security services and report to Parliament<sup>1335</sup> suggests that oversight will become more streamlined and have regard to human rights.

Despite its likely effectiveness and the safeguards outlined above, a number of

---

<sup>1331</sup> *ibid.*

<sup>1332</sup> *ibid* 170 (A9/1 Case Study).

<sup>1333</sup> Anderson D. *Legislation Report of the Bulk Powers Review* Cmd 9326 (HMSO, August 2016), 8 para. 120 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>> accessed June 2018.

<sup>1334</sup> *ibid*; UK Government *Investigatory Powers Bill Factsheet: Investigatory Powers Commission* (October 2015).

<sup>1335</sup> *ibid* UK Government Factsheet.

points have been raised about the Act's application and its proposals, which it is claimed, create unnecessary intrusion into private lives. For instance, Access Now, an international organisation which 'defends and extends digital rights globally',<sup>1336</sup> set out data privacy concerns about the Act's allowance for the Government to require ISPs to 'weaken or remove' encryption for surveillance purposes.<sup>1337</sup> Indeed, as the UN Special Rapporteur for the Promotion and Protection of the Right to Freedom of Opinion and Expression found, encryption and anonymity was a means to protect privacy, enabling specific groups such as journalists, civil society organisations, scholars, ethnic minorities, groups on sexual orientation and gender identity, as well as religious groups to exercise their rights to freedom of opinion and expression.<sup>1338</sup> There is ambiguity surrounding the Home Secretary's powers to regulate encryption, in particular, the potential for Internet Service Providers to maintain technology used to remove encryption of personal data under s. 253<sup>1339</sup>, stating that the vagueness of technical capability notices under that section could '*...could enable limitations on the development of strong encryption or the requirement to implement encryption back-doors...*'.<sup>1340</sup> By hampering the development of encryption data, Access Now claims that there will be a decrease trust in using the Internet, meaning that many will modify their behaviour and cease to share sensitive information, a point aggravated by the

---

<sup>1336</sup> Access Now <[www.accessnow.org](http://www.accessnow.org)> accessed November 2016.

<sup>1337</sup> Access Now *Written Evidence to the Public Bills Committee* IPB 72 (April 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm)> accessed November 2016.

<sup>1338</sup> *ibid*; Human Rights Council Twenty Ninth Session A/HRC/29/32 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (Office of the United Nations High Commissioner on Human Rights, 22 May 2015), 7-8, <[www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A.HRC.29.32\\_AEV.doc](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A.HRC.29.32_AEV.doc)> accessed November 2016.

<sup>1339</sup> NB. referred to within the evidence as Clause 217.

<sup>1340</sup> *ibid* Human Rights Council evidence.

geographical reach of the technical capability notices.<sup>1341</sup> Consequently, some of the encryption technical notices may in fact serve to dampen freedom of speech and expression over the Internet, potentially meaning that the Act will contradict existing human rights legislation – both nationally and internationally.

Similarly, there have been a number of concerns about the use of Internet Connection Records. As mentioned earlier, these have the potential to provide an effective means of identifying criminal conduct online and attributing it to an individual person. However, as noted by Liberty and other similar organisations,<sup>1342</sup> there is no need for a warrant for public authorities to access Internet Connection Records,<sup>1343</sup> creating an intrusive surveillance power which is not signed off by a judge and, similar to the metadata from email communications, these records can be kept for up to 12 months.<sup>1344</sup> Furthermore, the extent to which Internet Connection Records would apply is vast - as Liberty contend, “*in practice, ICRs would provide a detailed record of internet connections for every person in the UK*”<sup>1345</sup> which would comprise of a log of websites visited, system updates downloaded, every mobile app used and logs of any other device which was Internet-connected, including games consoles, digital

---

<sup>1341</sup> *ibid* Access Now *Written Evidence to the Public Bills Committee* IPB 72 (April 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm)> accessed November 2016.

<sup>1342</sup> E.g. Big Brother Watch; JUSTICE *Written Evidence to the Draft Investigatory Powers Bill Joint Committee* IPB0148 (HMSO, 17 December 2015) <[http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#\\_ftn21](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#_ftn21)> accessed November 2016.

<sup>1343</sup> Including Her Majesty’s Revenue and Customs, the Department for Work and Pensions, NHS Trusts and the Gambling Commission; Liberty *Liberty’s written evidence on the Investigatory Powers Bill* (March 2016), 22, paras. 43-44 – the only exception is local authorities - <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.

<sup>1344</sup> Investigatory Powers Act c.25, s. 87(11) – referred to in evidence as Clause 83(9).

<sup>1345</sup> *ibid* Liberty *Written Evidence*, 22-23, para. 47.

cameras and e-book readers.<sup>1346</sup> Coupled with the extent of records which can be accessed, is the potential for full website addresses to be identified under the Act. Although the UK Government stipulates that full web addresses could never be included in Internet Connection records, as “*under the law, this would be defined as content*”,<sup>1347</sup> concerns have been raised about the fact that particular domain names, such as *www.divorcesolicitors.com* can reveal far more about the user than generic websites, such as *www.google.co.uk*.<sup>1348</sup> Computers themselves, it is maintained, cannot determine the difference between content and non-content, therefore filters to safeguard privacy would be redundant.<sup>1349</sup> In this light, it is also telling that the US and the other “Five Eyes” nations mentioned by Snowden do not use mandatory retention of Internet Connection Records to identify illicit online activities.<sup>1350</sup> Indeed, as Anderson noted, “*such obligations were not considered politically conceivable by [his] interlocutors in Germany, Canada or the US*”<sup>1351</sup> and Australia specifically exempted web logs in its new data retention law in 2015.<sup>1352</sup> Consequently, this part of the Act would be an extremely intrusive form of surveillance and would potentially contradict both *Digital Rights Ireland* and Article 8 of the ECHR, as well as international human rights obligations.

---

<sup>1346</sup> *ibid.*

<sup>1347</sup> Home Office Factsheet *Investigatory Powers Bill: Internet Connection Records* (30 October 2015) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530556/Internet\\_Connection\\_Records\\_factsheet.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf)> accessed November 2016.

<sup>1348</sup> Lloyd, C. *Written evidence submitted to the Public Bills Committee* IPB 35 (HMSO, 24 March 2016) <<http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB35.htm>> accessed November 2016.

<sup>1349</sup> *ibid.*

<sup>1350</sup> NB. All the other ‘Five Eyes’ countries have written constitutions, therefore are bound by privacy aspects in those constitutions, whereas the UK, without a written constitution, can have a more elastic interpretation.

<sup>1351</sup> *ibid* Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 265, 14.30 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018.

<sup>1352</sup> *ibid.*

Perhaps the most controversial aspect of the Act is the continuance of bulk data collection and surveillance powers for the security services. As Anderson stated, the ‘extremely’ broad nature of the wording of ‘interception’ under s. 15(5) went further than his recommendations to allow thematic warrants for a specified organised crime group,<sup>1353</sup> meaning that the warrant would cover a large geographical area or collection of a large volume of data,<sup>1354</sup> stating that there was a need for targeted interception, rather than a more general approach.<sup>1355</sup> Despite an opportunity to narrow these powers, the Act continues to allow for bulk warrants – albeit with the added approval of a Judicial Commissioner.<sup>1356</sup> However, despite this improved safeguard, these powers may still be seen as inappropriate. For example, with bulk interception warrants,<sup>1357</sup> the Investigatory Powers Act’s limitation to ‘overseas communications’ will still capture communications where the sender or recipient is UK based, but is communicating with an overseas correspondent or is using an ‘external’ website or social media forum such as Google or Facebook.<sup>1358</sup> This potentially brings the Act into conflict with privacy rights enjoyed by UK, EU and US citizens. Furthermore, Anderson noted that the provision for national security notices under s. 252 of the Act mirrors s. 94 of the Telecommunications Act 1984, providing authority for the issuance of a notice “*requiring the operator to take such specified steps as the Secretary*

---

<sup>1353</sup> Anderson, D. *Written evidence to the Public Bills Committee* IPB 46 (March 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm)> accessed November 2016.

NB. This was referred to as Clause 15 within his evidence; s. 4 also defines interception.

<sup>1354</sup> *ibid.*

<sup>1355</sup> *ibid.*

<sup>1356</sup> Investigatory Powers Act c.25, s. 140, 159, 165, 179, 187, 208 and 216 on different bulk warrants all now require the approval by a Judicial Commissioner.

<sup>1357</sup> Investigatory Powers Act c.25, s. 136(2).

<sup>1358</sup> Investigatory Powers Act c.25, s. 136(5); Liberty *Liberty’s written evidence on the Investigatory Powers Bill* (March 2016), 44, para. 93 which refers to it as Clause 127 <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.



of State considers necessary in the interests of national security”<sup>1359</sup> meaning that there was too broad a definition of ‘national security’ for these to be applied appropriately.<sup>1360</sup> Snowden revealed that GCHQ used these powers for “*industrial scale exploitation*”<sup>1361</sup> using the broad ‘bulk’ warrant powers under s. 8 (1) and (4) of RIPA.<sup>1362</sup> Currently, there are only 15 ‘directions’, which allow intelligence agencies to collect bulk data,<sup>1363</sup> covering 50 billion data communications daily,<sup>1364</sup> and which currently only require the Home Secretary’s approval.<sup>1365</sup> The Act also does not take into account Anderson’s recommendations, including the fact that bulk collection of data (as happened with TEMPORA) should be subject to strict additional safeguards, including judicial authorisation,<sup>1366</sup> a tighter definition of the purposes for which it is sought,<sup>1367</sup> a targeting of communications of persons believed to be outside the UK,<sup>1368</sup> as well as a specific interception warrant to be judicially authorised if the applicant wishes to look at communications of a person believed to be within the UK.<sup>1369</sup>

---

<sup>1359</sup> *ibid* Anderson, D. *Written evidence to the Public Bills Committee* IPB 46 (March 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm)> accessed November 2016. NB. Within his evidence, it is referred to as Clause 216.

<sup>1360</sup> *ibid*.

<sup>1361</sup> According to Liberty, these were GCHQ’s own words; Liberty *Liberty’s written evidence on the Investigatory Powers Bill* (March 2016), 44, para. 91 <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.

<sup>1362</sup> *ibid* 44, para. 92.

<sup>1363</sup> Rt. Hon Sir Stanley Burton *Report of the Interception of Communications Commissioner, Review of Directions given under s94 of the Telecommunications Act 1984* (July 2016) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/548013/56208\\_HC33\\_WEB.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/548013/56208_HC33_WEB.pdf)> accessed June 2018; Bowcott, O. (The Guardian, 7 July 2016) *Fifteen secret warrants in force granting bulk data collection in UK* <<https://www.theguardian.com/law/2016/jul/07/fifteen-secret-warrants-in-force-granting-bulk-data-collection-in-the-uk>> accessed November 2016.

<sup>1364</sup> Liberty estimated in 2016, intelligence agencies were handling 50 billion communications per day; Liberty *Liberty’s written evidence on the Investigatory Powers Bill* (March 2016), 44, para. 92 <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.

<sup>1365</sup> Telecommunications Act 1984, s. 94.

<sup>1366</sup> *ibid* Anderson, D., 5, para. 14; Recommendation 22.

<sup>1367</sup> *ibid* Recommendation 43.

<sup>1368</sup> *ibid* Recommendation 44.

<sup>1369</sup> *ibid* Recommendation 79.

Therefore, some of the concerns raised by the intrusiveness of vast bulk data collection and interception warrants under RIPA do not seem to have been fully addressed by the Act.

The incompatibility of continuing bulk data collection and interception with recent decisions by the ECtHR also raises the question of the Act's appropriateness. In *Roman Zakharov v Russia*,<sup>1370</sup> the court stated that “[i]n view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse”,<sup>1371</sup> applying a necessity test to keep interference restricted to what is ‘necessary in a democratic society’.<sup>1372</sup> Whether large-scale surveillance techniques employed by GCHQ will be compatible with this judgement is debatable, untargeted bulk mobile phone surveillance in this case was deemed incompatible with Article 8 ECHR.<sup>1373</sup> However, in *Szabó and Vissy v Hungary*,<sup>1374</sup> the Fourth Section went further, stating that ‘strict necessity’ test was crucial with secret surveillance and must be subject to two criteria. Firstly, whether surveillance powers were key safeguarding democratic institutions. Secondly, whether the obtaining of information was key to an individual operation. Without testing strict necessity of such powers, the Court agreed, “any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal”.<sup>1375</sup> The development of the ‘strict necessity’ test in *Szabó* may be a significant barrier to the Act's operation, as the bulk data

---

<sup>1370</sup> *Roman Zakharov v Russia* (Application no. 47143/06) (Court (Grand Chamber)), [2015] ECHR 1065.

<sup>1371</sup> *ibid* [232].

<sup>1372</sup> *ibid*.

<sup>1373</sup> *ibid*.

<sup>1374</sup> *Szabó and Vissy v Hungary* (Application no. 37138/14) (Court (Fourth Section)), [2016] ECHR 579.

<sup>1375</sup> *ibid* [73].

warrants do not necessarily relate to individual cases, but may be part of a wider scale of data communications surveillance. In the Act's context, while there are judicial safeguards (unlike the mass surveillance laws of Hungary in *Szabó*), the fact that data retention and data surveillance technologies are so wide-ranging means that there is a danger that the Act's provisions will not be considered as appropriate by the ECHR.

Therefore, it is difficult to reconcile some of the Act's provisions with overarching EU legislation and the ECHR's principles of necessity and judicial intervention. Anderson also raised some questions regarding the 'dual lock' promised under the Act's provisions, noting that there was a need for involvement of judicial commissioners during each stage of the warrant process, as well as using counsel to act as amicus where appropriate in relation to applications for warrant approval.<sup>1376</sup> Anderson has also warned that the 'dual lock' may be abandoned in favour of approval by a senior official, even in the case of a major amendment to the warrant such as the addition of a new person or premises.<sup>1377</sup> Consequently, this highlights a major flaw in the appropriateness of the Act's protections for interception warrants. What is clear from the Investigatory Powers Act, is that it seeks to fill a gap created by the demise of the Data Retention Directive. However, in spite of the data privacy and freedom of

---

<sup>1376</sup> *ibid* Anderson, D. *Written Evidence to the Public Bills Committee*.

<sup>1377</sup> *ibid*.

expression concerns outlined above, in light of recent ISIL attacks in France and Belgium,<sup>1378</sup> as well as the result of the EU Referendum in June 2016,<sup>1379</sup> the Act reached Royal Assent in the Autumn of 2016.<sup>1380</sup>

### **5.2.3.a. The Investigatory Powers Act vs the CJEU**

Furthermore, the lack of an EU Data Retention Directive or similar surveillance structure raises questions on how such an Act and its provisions could be applied in co-operation with other EU Member States and be compatible with EU legislation. The High Court in the *Davis/Watson* case rejected the use of retained data and declared

---

<sup>1378</sup> On 14 July 2016, Mohamed Lahouaiej-Bouhlel drove a lorry into a crowd watching the Bastille Day fireworks in Nice, killing 84 people, BBC News (22 July 2016) *Nice lorry attack: Five suspected accomplices charged* <<http://www.bbc.co.uk/news/world-europe-36859312>> accessed November 2016; Palazzo, C. (The Telegraph, 21 July 2016) *Islamic State threatens to intensify attacks against France* <<http://www.telegraph.co.uk/news/2016/07/21/islamic-state-threatens-to-intensify-attacks-against-france/>> accessed November 2016; on 22 March 2016, 32 people were killed and 340 injured when simultaneous bombs were set off at Zaventem International Airport and Maelbeek Metro Station, with Mohamed Abrini later arrested and charged; BBC News (9 April 2016) *Brussels explosions: What we know about airport and metro attacks* <<http://www.bbc.co.uk/news/world-europe-35869985>> accessed November 2016; on 13 November 2015, co-ordinated attacks in Paris claimed the lives of 130 people and injured a further 368. ISIL claimed responsibility; Castillo, M., Haddad, M., Martinez, M. & Almasy, S. (CNN, 16 November 2016) *Paris suicide bomber identified; ISIS claims responsibility for 129 dead* <<http://edition.cnn.com/2015/11/14/world/paris-attacks/>> accessed November 2016. The two surviving perpetrators, Salah Abdeslam and Mohamed Abrini, have both been arrested and charged (Abrini is awaiting extradition to France from Belgium after the Brussels attack); BBC News (20 May 2016) *Paris attacks: Salah Abdeslam stays silent in French court* <<http://www.bbc.co.uk/news/world-europe-36340739>> accessed November 2016; BBC News (9 June 2016) *Paris attacks: Mohamed Abrini to be extradited to France* <<http://www.bbc.co.uk/news/world-europe-36492309>> accessed November 2016.

<sup>1379</sup> The UK voted to leave the European Union on 23 June 2016 by 51.9% to 48.1%; Electoral Commission *EU referendum results* (June 2016) <<http://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information>> accessed November 2016.

NB. The UK is still bound by EU law and the judgements of the CJEU until it exits the European Union or two years from its notification to leave the EU – see Article 50(1), (2) and (3) of the Lisbon Treaty.

<sup>1380</sup> The Act received Royal Assent on 29 November 2016 <<https://services.parliament.uk/bills/2015-16/investigatorypowers.html>> accessed June 2018.

DRIPA invalid, something which is likely to be followed by the CJEU when it provides its full judgement on *Home Secretary v Watson and Others*.<sup>1381</sup> An initial opinion<sup>1382</sup> by the CJEU's Advocate General, Henrik Saugmandsgaard ØE indicates that the CJEU would reject an obligation for an electronic communication service provider to generally retain data as incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, 'The Charter', unless certain criteria were satisfied.<sup>1383</sup> Instead, as the opinion notes, Member States must ensure that the obligation would include legislative or regulatory measures which allow foreseeability, accessibility and adequate protection against arbitrary interference,<sup>1384</sup> as well as an observance of Articles 7 and 8 of The Charter. Furthermore, the use of retained data must be 'strictly necessary' in the fight against serious crime, that is, no other measure or combination of measures could be as effective,<sup>1385</sup> and must include all of the safeguards described in *Digital Rights Ireland*. Finally, and most importantly, the legislation or regulation for retained data must be "*proportionate, in aa democratic society, to the objective of fighting serious crime*"<sup>1386</sup> meaning that the serious risks to privacy and data protection of the majority of law abiding citizens must not be disproportionate to the significant advantages of data retention in the fight against serious crime.<sup>1387</sup>

---

<sup>1381</sup> Case C-698/15 *Home Secretary v Tom Watson, Peter Brice, Geoffrey Lewis – Intervening Parties: Open Rights Group, Privacy International, The Law Society of England and Wales*.

NB. As David Davis MP is now a Government Minister, he is now unable to challenge the UK Government through the courts.

<sup>1382</sup> Opinion by Henrik Saugmandsgaard ØE Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15)*, (19 July 2016) <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=391253>> accessed November 2016.

<sup>1383</sup> *ibid* [263].

<sup>1384</sup> *ibid*.

<sup>1385</sup> *ibid*.

<sup>1386</sup> *ibid*.

<sup>1387</sup> *ibid*.

This issue of proportionality is also reflected in the Convention on Cybercrime’s Article 15, whereby it outlines that domestic law will “*incorporate the principle of proportionality*” to balance human rights requirements.<sup>1388</sup> Furthermore, it is telling that the US Congress passed the USA Freedom Act of 2015,<sup>1389</sup> forcing authorisation of bulk metadata collection by the NSA under §215 of the USA PATRIOT Act to lapse, with bulk surveillance under §702 of the Foreign Intelligence Surveillance Act (FISA) due to expire in 2017,<sup>1390</sup> potentially being replaced with more targeted access to records. In particular, there are now prohibitions on bulk collection of pen register, as well as trap and trace devices under FISA,<sup>1391</sup> and National Security Letters.<sup>1392</sup> Consequently, it is clear that the Investigatory Powers Act will have to adhere to both the CJEU’s decision and be compatible with other countries’ views on bulk collection, such as the US, in order to be both effective and appropriate.

#### **5.2.3.b. The Investigatory Powers Act vs The Data Protection Directive 2016**

In 2016, the European Commission introduced a new data protection Directive,<sup>1393</sup> to be applied by Member States by 2018.<sup>1394</sup> This provides for further protections on the

---

<sup>1388</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), Article 15(1).

<sup>1389</sup> Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (“USA Freedom Act”) (Pub. L. 114-23, 120 Stat 200) (50 U.S.C. 1801).

<sup>1390</sup> Singh Guliani, N. (ACLU Legislative Counsel) *What’s Next for Surveillance Reform After the USA Freedom Act* (ACLU Blog, 3 June 2015) <<https://www.aclu.org/blog/washington-markup/whats-next-surveillance-reform-after-usa-freedom-act>> accessed November 2016.

<sup>1391</sup> §201 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (“USA Freedom Act”) (Pub. L. 114-23, 120 Stat 200) (50 U.S.C. 1801).

<sup>1392</sup> *ibid* §501.

<sup>1393</sup> Directive 2016/680/EU (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>1394</sup> This Directive must be introduced by 6 May 2018 <<http://ec.europa.eu/justice/data-protection/>> accessed 19 August 2016.

processing of personal data by Member States when investigating criminal offences. This will replace existing data protection legislation in EU Member States, including the UK's Data Protection Act 1998. For instance, the Directive and accompanying General Data Protection Regulations outline clear principles for data protection processing under Article 5,<sup>1395</sup> including data collection for specific, explicit and legitimate purposes<sup>1396</sup> and limitation of identification of data subjects for 'no longer than is necessary'.<sup>1397</sup> Furthermore, the Directive clearly highlights that the data protection principles should apply when the communications can identify a data subject,<sup>1398</sup> bringing it into line with the *Digital Rights Ireland* decision. Finally, breaches of the Directive and Regulations carry a more significant fine for data controllers than the Data Protection Directive or the Data Protection Act 1998<sup>1399</sup> – now €20 million or 4% of annual global turnover for the preceding year.<sup>1400</sup> Despite the fact that there are exemptions to the data processing regulations in terms of national security,<sup>1401</sup> public security<sup>1402</sup> and the "*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and*

---

<sup>1395</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/6/EC (General Data Protection Regulation). See Article 5(1) of the Regulations.

<sup>1396</sup> *ibid.*

<sup>1397</sup> *ibid.*

<sup>1398</sup> Directive 2016/680/EU (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, para. 24.

<sup>1399</sup> General Data Protection Regulation Article 83(5); The maximum fine for breaches of the Data Protection Act 1998 c.29 is currently £500,000 through the Information Commissioner's Office <<https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/>> accessed November 2016; Criminal Justice and Immigration Act 2008 c.4, s. 144 as amended, which amends s.55 of the Data Protection Act 1998 c.29 on monetary penalties for data controllers.

<sup>1400</sup> *ibid* Directive 2016/680/EU (27 April 2016) on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Articles 12-17.

<sup>1401</sup> *ibid* Directive 2016/680/EU Article 23(1)(a).

<sup>1402</sup> *ibid* Directive 2016/680/EU Article 23(1)(c).

*the prevention of threats to public security*”,<sup>1403</sup> these are limited to what is constituted as a “*necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned*”.<sup>1404</sup> The Directive also places strict restrictions on the transfer of data to third countries outside of the EU,<sup>1405</sup> including whether the transfer is necessary, prior permission from another Member State if the data is made available from that Member State or an adequacy decision from the European Commission,<sup>1406</sup> potentially neutralising the actions carried out by GCHQ and the NSA in TEMPORA and PRISM. Therefore, it is not difficult to surmise that telecommunications providers will become more reluctant to share information relating to a terrorism offence for fear of a fine which could ruin their business, thereby hampering effectiveness of legislation such as the Investigatory Powers Act. While the EU is taking the path of further safeguarding individual rights to privacy, the UK has increased its surveillance capabilities, creating concern as to the compatibility of the Investigatory Powers Act with EU law and whether it can be applied across other Member States without breaching both settled judgement and recent EU legislation.

### **5.3. Legitimate Sources of Finance**

As with the US, this is a significantly difficult area for the UK to successfully and appropriately monitor. The rise of ‘lone wolf’ terrorist attacks since 9/11 and cheap terrorism also makes it harder for law enforcement agencies to be able to track and trace small amounts being channelled through the Internet. As in chapter four, this

---

<sup>1403</sup> *ibid* Directive 2016/680/EU Article 23(1)(d).

<sup>1404</sup> *ibid* Directive 2016/680/EU, [26].

<sup>1405</sup> *ibid* Directive 2016/680/EU, Article 35(2).

<sup>1406</sup> *ibid* Article 35(1).



section examines the two main ways of raising and channelling terrorist finances via legitimate sources, through charities and the global financial system, as well as examining the measures the UK uses to counteract cheap terrorism, including PREVENT.

### 5.3.1. Charities

Following 9/11, the UK used similar tactics to the US in order to prevent terrorist financing from being raised over the Internet when charities are used as a front. For example, as noted in chapter three, the Terrorism Act 2000 had a number of provisions to counteract the financing of terrorism through charities, including the duty of employees to disclose information if they have suspicion of terrorist financing offences during the course of business under s19.<sup>1407</sup> Additionally, ATCSA enabled HM Treasury to issue freezing orders against charities if their cash is intended to be used for the purposes of terrorism.<sup>1408</sup> However, this is restricted to where HM Treasury can reasonably believe “*that there is a specified threat to UK nationals, UK residents or the UK economy, and only when that threat emanates from a foreign government or foreign resident*”,<sup>1409</sup> thereby limiting its reach. Furthermore, UK based charities were required to register with the Charity Commission,<sup>1410</sup> and are subject to monitoring requirements.<sup>1411</sup> The Charity Commission also aims to provide law enforcement with

---

<sup>1407</sup> Terrorism Act 2000, c.11 Part III, s. 19 and s. 15-18.

<sup>1408</sup> Anti-terrorism Crime and Security Act 2001 c.24, s. 1, s. 4.

<sup>1409</sup> Anti-terrorism, Crime and Security Act 2001 c.24, s. 4(2); Anderson D. *First Report on the Operation of the Terrorist-Asset Freezing etc. Act 2010* (HMSO, December 2011), 10 <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/223465/fin\\_sanc\\_report\\_on\\_terrorist\\_asset\\_freezing\\_151211.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/223465/fin_sanc_report_on_terrorist_asset_freezing_151211.pdf)> accessed June 2018.

<sup>1410</sup> HM Treasury *Combating the financing of terrorism – A Report on UK Action* (October 2002) <[http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating\\_terrorism.pdf](http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating_terrorism.pdf)> accessed November 2016.

<sup>1411</sup> For example, charities are required to provide annual accounts, and the Charity Commission monitors charities if they work in high risk areas or carry out high risk activities. With regard to counter-terrorism, the Charity Commission has four strands within its Counter-Terrorism Strategy; Charity Commission *The Charity Commission's counter-terrorism work* (23 May 2013)

valuable information about charitable links with terrorism.<sup>1412</sup> However, the effectiveness of its co-operation was criticised in the wake of the 2005 London bombings (“7/7”). After the bombings, it was found that Mohammed Siddique Khan and Shehzad Tanweer were former trustees of a registered charity and running a bookshop on behalf of, Iqra, a charity registered in 2003,<sup>1413</sup> and which held £12,500 of charitable funds in four bank accounts.<sup>1414</sup> A further two alleged to have been involved in the 7/7 bombings, Khalid Khaliq and Waheed Ali, were trustees of this charity, although Ali was later cleared of any involvement and Khaliq was imprisoned after admitting he possessed an al-Qaeda manual on a computer CD.<sup>1415</sup> Although there was no evidence to suggest that the charity’s funds had been used for 7/7, there were considerable concerns that it had not filed accounts with the Commission, despite an income of £94,000 since its registration.<sup>1416</sup> Furthermore, Iqra’s bookshop had been used by the 7/7 bombers to meet with each other and plan their acts, and had sold extremist literature, which was subsequently found by police to have made up one fifth

---

<<https://www.gov.uk/government/publications/the-charity-commissions-counter-terrorism-work/the-charity-commissions-counter-terrorism-work>> accessed November 2016.

<sup>1412</sup> E.g. Crescent Relief (2006); Balls, E. (former Economic Secretary to the Treasury) *Written Statement* (Hansard, 10 October 2006)

<<https://publications.parliament.uk/pa/cm200506/cmhansrd/vo061010/wmstext/61010m0001.htm>>

accessed April 2018; Palestinians Relief Fund (Interpal) (2003), although unfroze assets; Charity Commission *Palestinians Relief and Development Fund (Interpal)* (27 February 2009)

<<http://www.charity-commission.gov.uk/investigations/inquiryreports/interpal.asp>> accessed November 2016; Cutbill, C. *The money launderer, the terrorist financier the charity and the law* (2005) 2 Private Client Business 100, 101; Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283, 287.

<sup>1413</sup> Charity Commission *Iqra* (22 February 2011) <<https://www.gov.uk/government/publications/archived-inquiry-reports/archived-inquiry-reports#inquiry-reports-published-in-2011>> accessed November 2016.

<sup>1414</sup> *ibid.*

<sup>1415</sup> *ibid*; *R v Waheed Ali* [2009] EWCA Crim 2396; BBC News (28 April 2009) *Trio cleared over 7/7 attacks* <<http://news.bbc.co.uk/1/hi/uk/7507842.stm>> accessed November 2016; *R v K* [2008] 2 WLR 1026, [2008] EWCA Crim 185; Wainwright, M. (The Guardian, 12 March 2008) *Friend of 7/7 bombers jailed for possessing al-Qaida CD* <<https://www.theguardian.com/uk/2008/mar/12/uksecurity.alqaida>> accessed November 2016.

<sup>1416</sup> *ibid* Charity Commission *Iqra* (22 February 2011) <<https://www.gov.uk/government/publications/archived-inquiry-reports/archived-inquiry-reports#inquiry-reports-published-in-2011>> accessed November 2016.

of the literature held at the premises.<sup>1417</sup> Consequently, the Charity Commission found, six years after the event, that mismanagement of the charity had occurred, with a failure to “*properly manage material available to the public at the Charity’s premises*”,<sup>1418</sup> leading to concerns that legitimate charities were still being infiltrated by extremists and terrorists, despite the efforts of national Government after 9/11.

It was also found by the resulting investigation that no fewer than 8 charities had direct or indirect links to the 7/7 bombings,<sup>1419</sup> and closer work between the Charity Commission and law enforcement authorities was called for after it was found that 48 Suspicious Activity Reports<sup>1420</sup> had been filed regarding these charities.<sup>1421</sup> Out of these, 34 warranted further investigations.<sup>1422</sup> Consequently, the Charity Commission published its Counter Terrorism Strategy,<sup>1423</sup> which included preventative measures, such as annual reporting,<sup>1424</sup> disrupting finances<sup>1425</sup> and using “zero tolerance” for charities involved in terrorist activities.<sup>1426</sup> Furthermore, the Charity Commission

---

<sup>1417</sup> *ibid.*

<sup>1418</sup> *ibid.*

<sup>1419</sup> Ryder N. *Terror funds – charities and the funding of terrorism – where does your money go?* (2007) *New Law Journal* 157 (7289), 1305, 1306.

<sup>1420</sup> See Chapter Three for further information; Suspicious Activity Reports are a crucial plank of national and international counter-terrorist financing measures.

<sup>1421</sup> Travis, A. (The Guardian, 11 May 2007) *Warning on Terrorist Charity* <<http://www.guardian.co.uk/uk/2007/may/11/terrorism.voluntarysector>> accessed November 2016; HM Treasury and Home Office consultation summary responses *Review of the Safeguards to Protect the Charitable Sector (England and Wales) from terrorist abuse* (December 2007) <<http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-2007-protecting-charities/cons-2007-charities-responses?view=Binary>> accessed November 2016.

<sup>1422</sup> *ibid.*

<sup>1423</sup> Charity Commission *Counter Terrorism Strategy* (July 2008) <<https://www.gov.uk/government/collections/charity-commission-reports-decisions-alerts-and-statements>> accessed April 2018; Charity Commission Operational Guidance about charities and terrorism <<http://ogs.charitycommission.gov.uk/g410a001.aspx>> accessed April 2018; Charities Act 2006 c.50.

<sup>1424</sup> *ibid* Charity Commission’s Operational Guidance about charities and terrorism, 16.

<sup>1425</sup> *ibid* 13.

<sup>1426</sup> *ibid.*

provided guidance for charities regarding terrorist financing<sup>1427</sup> and conducted inquiries into suspicious activities or donations.<sup>1428</sup> Moreover, HM Revenue and Customs assisted the Charity Commission by providing some funding for its counter-terrorism strategy.<sup>1429</sup> Therefore, the Charity Commission had been provided with more powers in order to make its investigations more effective.

After a change of Government, these requirements were consolidated into the Charities Act 2011, with a requirement for charities to register with the Charity Commission under s. 29 and s. 30,<sup>1430</sup> and powers for the Charity Commission to institute inquiries into individual charities,<sup>1431</sup> with evidence being taken under oath<sup>1432</sup> and the power to obtain search warrants for the purposes of inquiry,<sup>1433</sup> potentially heightening the Charity Commission's effectiveness in finding charities which have been involved or infiltrated by terrorist organisations. Furthermore, charities are now obliged to keep accounting records for at least six years,<sup>1434</sup> providing the Charity Commission and law enforcement authorities with an opportunity to scrutinise accounts and potentially prevent charity involvement in the raising and channelling of terrorist finances.

However, several terrorist and extremist activities linked with charitable donations emerged in 2012 and 2013. For example, Irfan Naseer, Irfan Khalid and Ashik Ali were found guilty of fraudulently raising over £12,000 during the Muslim fasting month of Ramadan behind the front of a legitimate registered charity, Muslim Aid, with most of its finances going towards a prevented terrorist attack in Birmingham in

---

<sup>1427</sup> *ibid.*

<sup>1428</sup> Charity Commission Reports <<https://www.gov.uk/government/collections/inquiry-reports-charity-commission>> accessed November 2016.

<sup>1429</sup> *ibid* Charity Commission, *Counter Terrorism Strategy*, 17.

<sup>1430</sup> Charities Act 2011 c. 25.

<sup>1431</sup> Charities Act 2011 c.25, s. 46.

<sup>1432</sup> *ibid* s. 47.

<sup>1433</sup> *ibid* s. 48.

<sup>1434</sup> *ibid* s. 131.

2011.<sup>1435</sup> Although it was established that Muslim Aid had no links with the terrorist plot,<sup>1436</sup> other charities have expressed sympathies for acts of terror and, in 2012, it was alleged that the Camden Abu-Dis Friendship Association had expressed support for suicide bombers in Palestine on its website, referring to them as ‘martyrs’, ‘killed by Zionists’,<sup>1437</sup> with its Chairman Munir Nusseibeh allegedly publicly expressing support for Khader Adnan, a jailed terrorist leader of the Palestinian Islamic Jihad, a proscribed terrorist organisation in the UK,<sup>1438</sup> on Iranian Press TV.<sup>1439</sup> Furthermore, in 2012, concerns were raised that the Al-Muntada El-Islami Trust had been linked to financing the al-Qaeda inspired group Boko Haram in Nigeria.<sup>1440</sup> In 2013, the Na-

---

<sup>1435</sup> *R v Irfan Khalid and others* (2013); NB. Ali pleaded guilty in 2012. The charity Muslim Aid had no knowledge of this fundraising and only received £1,500 of the donations raised. In fact, the convicted were ordered to pay back more than £33,000 to the charity in 2014; BBC News (13 January 2014) *Men told to repay Birmingham terror plot cash* <<http://www.bbc.co.uk/news/uk-england-birmingham-25703118>>, accessed November 2016.

<sup>1436</sup> NB. Muslim Aid allegedly admitted that it had donated to the charity Al-Ihsan, which is connected to two terrorist organisations, the Palestinian Islamic Jihad and the Islamic School of Gaza; Gilligan A. (The Telegraph, 25 December 2010) *Charity Watchdog loses its bite* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8225028/Charity-watchdog-loses-its-bite.html>> accessed November 2016; but the Charity Commission found that it had no links to these organisations in 2010, Charity Commission *Regulatory Case Report (2010) Muslim Aid* <<https://www.gov.uk/government/publications/archived-case-reports/archived-case-reports#regulatory-case-reports-published-in-2010>> accessed November 2016. Muslim Aid now has an interim manager appointed by the Charity Commission, subject to s. 84 Charities Act 2011 c.25; Charity Commission *Charity Commission names further charities under investigation* (5 June 2014) <<https://www.gov.uk/government/news/charity-commission-names-further-charities-under-investigation>> accessed November 2016; Charity Commission *Interim Manager appointed to Muslim Aid* (21 October 2016) <<https://www.gov.uk/government/news/interim-manager-appointed-to-muslim-aid>> accessed November 2016.

<sup>1437</sup> Stand for Peace, *Camden Abu Dis Friendship Association* (24 September 2012) <<http://standforpeace.org.uk/camden-abu-dis-friendship-association/>> accessed November 2016.

<sup>1438</sup> The Home Office listed this as a proscribed organisation in 2001; Home Office *Proscribed Terrorist Organisations* (15 July 2016) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/538297/20160715-Proscription-website-update.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538297/20160715-Proscription-website-update.pdf)> accessed November 2016.

<sup>1439</sup> *ibid* Stand for Peace.

<sup>1440</sup> Doward, J. (The Guardian, 9 September 2012) *Peer raises fears over UK charity's alleged links to Boko Haram* <<https://www.theguardian.com/world/2012/sep/09/uk-charity-boko-haram>> accessed November 2016. This is linked with later evidence provided by Emmanuel Ogebe Esq. to the U.S. House of Representatives Foreign Affairs Committee in 2013; *Testimony of Mr. Emmanuel Ogebe, Esq. On Behalf of the Jubilee Campaign On The Rising Global Threat of Boko Haram& US Policy Intransigence Before the Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations and the Subcommittee on Terrorism, Nonproliferation, and Trade, Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations*, 11 (13 November 2013) <<https://oversight.house.gov/wp-content/uploads/2014/09/Mr.-Ogebe-Statement-Bio.pdf>>

tional Audit Office (NAO) assessed the Charity Commission’s regulatory effectiveness,<sup>1441</sup> highlighting that the Charity Commission had made poor use of its investigatory powers and failed to take tough action in some cases.<sup>1442</sup> Furthermore, the NAO found that the Commission had been slow to act in one case, initially hearing concerns about the charity in 2003 and then conducting no fewer than four separate investigations between 2003 and 2009, finally installing an interim manager in 2010.<sup>1443</sup> Additionally, the NAO found that the Commission’s information gathering powers had significantly declined between 2008 and 2013, and instead of using its powers to receive bank statements directly from the bank, it “*now asks [trustees] for bank statements*”.<sup>1444</sup> Notably, the Commission’s monitoring cases dropped from 200 per year in 2008-2009 to just 42 in 2012-13.<sup>1445</sup> Thus, despite the powers it had been granted, the Charity Commission had been slow to act in several investigations, potentially putting some charities at risk of infiltration by terrorist cells, as well as hampering the effectiveness of law enforcement authorities to act if a charity had been involved in supporting proscribed groups.

Since the NAO’s report, the Charity Commission has been more effective in investigating charities by changing its business model and focusing on charities at ‘high risk’.<sup>1446</sup> Furthermore, it increased the amount of statutory inquiries from 15 in

---

accessed November 2016. The Charity Commission started to investigate in 2012 whether the Al-Muntada El-Islami Trust was the same as those referenced in connection with Boko Haram – see Doward J. above. However, nothing has been heard since.

<sup>1441</sup> National Audit Office *The regulatory effectiveness of the Charity Commission* HC 813 Session 2013-14 (4 December 2013) <<https://www.nao.org.uk/report/regulatory-effectiveness-charity-com-mission-2/>> accessed November 2016.

<sup>1442</sup> *ibid.*

<sup>1443</sup> *ibid.* 34.

<sup>1444</sup> *ibid.* 37.

<sup>1445</sup> *ibid.*

<sup>1446</sup> National Audit Office, *Follow up on the Charity Commission*, HC 908 Session 2014-15 (22 January 2015) <<https://www.nao.org.uk/report/follow-up-on-the-charity-commission/>> accessed November 2016.

2012-13 to 64 in 2013-14<sup>1447</sup> and used information-gathering powers 652 times in 2013-14 compared with 200 in 2012-13.<sup>1448</sup> This has led to a more proactive stance by the Charity Commission, leading to a more effective model of investigating charities with terrorist links. For example, the Charity Commission in July 2016 struck off two charitable trusts set up by Adeel Ulhaq, after it was found that he had potentially channelled financing to ISIL jihadists in Syria through the trusts.<sup>1449</sup> Despite this progress, it remains to be seen whether the Charity Commission can continue to improve its use of investigatory powers to root out charities which have supported terrorist causes.

The effectiveness of the Charity Commission and law enforcement authorities' investigations into charities is also hampered, as with the US, because UK legislation and guidance is limited by territorial provisions, which does not resolve the problems Internet-based charities pose, and meaning a reliance on international co-operation to fulfil the aim of preventing and suppressing terrorist financing.<sup>1450</sup> Instead, the Charity Commission is again required to provide guidance regarding the conduct of charities working internationally.<sup>1451</sup> To compound this issue further, the Financial Action Task Force (FATF) has recently changed its guidance towards the regulation of charities. In June 2016, the FATF removed the wording that Non-Profit Organisations

---

<sup>1447</sup> *ibid* 8.

<sup>1448</sup> *ibid*.

<sup>1449</sup> Charity Commission Inquiry *Funds raised for charitable purposes and held on charitable trusts in the name of Adeel Ulhaq* (28 July 2016) <<https://www.gov.uk/government/publications/charitable-funds-raised-by-mr-adeel-ul-haq-inquiry-report>> accessed June 2018, in which the Commission found that some donations raised for humanitarian assistance was being spent pieces of equipment, with a significant proportion of £12,000 of donations being unaccounted for. Ul-Haq himself was convicted of terrorism offences in 2016; Crown Prosecution Service *R v Forhad Rahman, Adeel Brekke and Kaleem Kristen Ulhaq* (November 2016) <<https://www.cps.gov.uk/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-end-2006>> accessed November 2016.

<sup>1450</sup> Chapter one, 1.4.2.1.

<sup>1451</sup> Charity Commission *Charities: how to manage risks when working internationally*, (10 May 2013) <<https://www.gov.uk/guidance/charities-how-to-manage-risks-when-working-internationally>> accessed November 2016; Charity Commission *Charities and Terrorism: Compliance Toolkit* <<https://www.gov.uk/government/publications/charities-and-terrorism>> accessed November 2016.

(NPOs) were ‘*particularly vulnerable*’ to abuse by terrorist organisations from Recommendation 8.<sup>1452</sup> Potentially, this could create a conflict as to how the Charity Commission, financial institutions and the Government, as well as law enforcement in other countries can effectively fulfil their obligations to monitor and investigate charities suspected of terrorist financing over the Internet, and to ensure that high risk charities receive the support and monitoring they need. Consequently, more clarity and uniformity with international co-operation or guidance is needed to carry out measures to prevent Internet charities from being open to abuse by terrorist organisations.

To counteract concerns about the lack of territorial reach, the Terrorism Act 2000 places the onus on donors, only providing a defence under s. 18(2); that the donor did not have reasonable cause to know or suspect that the “arrangement” was related to terrorist property,<sup>1453</sup> acting as a strong deterrent for donors who would potentially fund terrorist causes. However, the appropriateness of this stance has been criticised on the basis that it is more difficult to substantiate than other crimes such as money laundering.<sup>1454</sup> For example, if donors are not aware that another part of the charity is channelling resources into terrorist acts, it may be difficult to prove that they were unaware of providing material property to a terrorist cause. The lowering of the standard of proof to a civil rather than a criminal standard relating to property allowing the state to “*divest individuals suspected, but not convicted, of terrorist activity of their*

---

<sup>1452</sup> Financial Action Task Force *Outcomes of the Plenary meeting of the FATF, Busan Korea* (22–24 June 2016) <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html>> accessed November 2016; Financial Action Task Force Recommendation 8 <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed November 2016.

<sup>1453</sup> Terrorism Act 2000 c.11, s. 18; *ibid* Cutbill, C. *The money launderer, the terrorist financier the charity and the law* (2005) 2 Private Client Business 100, 104.

<sup>1454</sup> *ibid* Cutbill, C., 104.



property”<sup>1455</sup> is of some concern, replicated in ATCSA 2001, whereby assets are frozen *from the start* of the investigation.<sup>1456</sup>

Criticisms about issuing freezing orders from the beginning of investigations were reflected in the case of *HM Treasury v Ahmed and others*.<sup>1457</sup> Here, the Supreme Court found that the UK Government’s Terrorism (United Nations Measures) Order 2006 was *ultra vires* and ordered it to be quashed.<sup>1458</sup> Under the Order, assets could be frozen, apart from basic expenses, if the Treasury had designated a person that they “*have reasonable grounds for suspecting*”<sup>1459</sup> of supporting terrorism. Unlike ATCSA 2001, where freezing orders were subject to Parliamentary scrutiny,<sup>1460</sup> Article 4 of the Order lays the power to designate persons firmly with HM Treasury alone, enabling it to freeze a person’s assets without Parliamentary scrutiny.<sup>1461</sup> In this instance, HM Treasury had not used its asset freezing powers under ATCSA 2001, but instead relied on the United Nations Act 1946, which provides Ministers with a general authorisation to make such Orders as are ‘*necessary or expedient*’ to give effect to Security Council Resolutions,<sup>1462</sup> and circumvented Parliamentary scrutiny of such freezing orders. The Court further held that the general wording s. 1 of the United

---

<sup>1455</sup> Donohue, L. K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int’l L 303, 409.

<sup>1456</sup> Anti-terrorism, Crime and Security Act 2001 c.24, s. 4(1); Elagab, O. *Control of Terrorist Funds and the banking system* (2006) 21(1) Journal of International Banking Regulation 38, 42; Justice Collins, A v *Her Majesty’s Treasury* [2008] 2 C.M.L.R. 44 – see below for the appeal in *HM Treasury v Ahmed and others* [2010] UKSC 2.

<sup>1457</sup> *HM Treasury v Mohammed Jabar Ahmed and others; Her Majesty’s Treasury v Mohammed al-Ghabra; R (on the application of Hani El Sayed Sabaei Youssef) v Her Majesty’s Treasury* [2010] UKSC 2.

<sup>1458</sup> *ibid*.

<sup>1459</sup> *ibid* *HM Treasury v Ahmed and others*; Terrorism (United Nations Measures) Order 2006 SI 2006/2657, Article 4(1)(2).

<sup>1460</sup> Anti-terrorism, Crime and Security Act c.24, s. 10(2).

<sup>1461</sup> Terrorism (United Nations Measures) Order 2006 SI 2006/2657, Article 4.

<sup>1462</sup> United Nations Act 1946 c. 45 (Regnal 9 and 10 Geo 6) s. 1(1).

Nations Act 1946, did not have explicit language contained therein to override fundamental human rights such as the right to a private life.<sup>1463</sup> Therefore, the Order's inclusion of "reasonable grounds for suspecting" went further than either the Act or the Resolution had intended, causing egregious circumstances for those designated under the Order. This stance has been reflected in cases in the US, such as *KindHearts for Charitable Humanitarian Development Inc v Timothy Geithner et al.*<sup>1464</sup> Here, the US District Court for the Northern District of Ohio found that the withholding of access to assets to pay counsel's fees had been 'arbitrary' and 'capricious'.<sup>1465</sup> The Government needed a warrant based on probable cause before freezing an organisation's assets.<sup>1466</sup> The Supreme Court in *Ahmed* also mentioned that the CJEU held in *Kadi v Council of the European Union*,<sup>1467</sup> that the listing process under Council Regulation (EC) No 881/2002 on the freezing of assets was incompatible with human rights, as Community authorities were bound to communicate the grounds on which an inclusion on the asset-freezing list is based to the people or entities concerned, therefore annulling it.<sup>1468</sup> Additionally, the ECtHR took a similar stance to *Kadi* in the 2013

---

<sup>1463</sup> For example, Article 8 of the European Convention on Human Rights; that of the right to respect one's private and family life. In the joined case of *Hani El Sayed Sabaei Youssef*, it was found that he had been denied access to funds since September 2005, only being supported by his wife who, under licence from the Treasury, could access welfare benefits. However, she could only spend money on 'basic expenses', as determined by the Treasury and was required to report to the Treasury on every item of household expenditure, including that of her children. *ibid Ahmed and others* [39], [137].

<sup>1464</sup> *KindHearts for Charitable Humanitarian Development Inc v. Timothy Geithner et al.* Case 3:08-cv-02400 (18 August 2009). The Ohio court held that the Government had violated its right to due process by freezing assets without notice and that the Government needed to obtain a warrant based on probable cause before freezing an organisation's assets <<https://www.aclu.org/cases/kindhearts-charitable-humanitarian-development-inc-v-geithner-et-al>> accessed November 2016.

<sup>1465</sup> *ibid*; also see *HM Treasury v Mohammed Jabar Ahmed and others; Her Majesty's Treasury v Mohammed al-Ghabra; R (on the application of Hani El Sayed Sabaei Youssef) v Her Majesty's Treasury* [2010] UKSC 2 [70].

<sup>1466</sup> *ibid*.

<sup>1467</sup> Joined Cases C-402/05 P and C-415/05 P *Kadi v Council of the European Union and Commission of the European Communities* (2008).

<sup>1468</sup> *ibid*. The final judgement of the Grand Chamber stated that it: *Annuls Council Regulation (EC) No 881/2002 of 27 May 2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaeda network and the Taliban, and repealing Council Regulation (EC) No 467/2001 prohibiting the export of certain goods and services*

case of *Al-Dulimi and Montana Management Inc. v Switzerland*,<sup>1469</sup> finding that the appellants “*sustained major restrictions*” as their assets had been frozen as far back as 1990, with the confiscation decision only being conferred in 2006<sup>1470</sup> and holding that there had been a breach of Article 6(1) of the ECHR, or the right to a fair trial.<sup>1471</sup> Consequently, although freezing assets from the beginning of an investigation is potentially an effective tool, charities and individual donors who are subject to an investigation had little ability to access any resources until the investigation is over, or access adequate redress, creating concerns similar to those of US provisions against US-based Muslim charities. Thus, the UK’s methods of disrupting terrorist finances through asset freezing orders did not balance civil liberties with national security effectively.

Since the case of *HM Treasury v Ahmed*, the Government introduced the Terrorist Asset Freezing etc. Act 2010, which is intended to address some of the concerns raised by *Ahmed*, by significantly increasing the burden of law enforcement authorities to prove reasonable suspicion, through replacing the wording of ‘*is or may be a person who commits, attempts to commit, participates in or facilitates the commission of acts of terrorism*’<sup>1472</sup> with a tougher test of whether HM Treasury reasonably believes “*that the person is or has been involved in terrorist activity*”.<sup>1473</sup> This therefore raises

---

*to Afghanistan, strengthening the flight ban and extending the freeze of funds and other financial resources in respect of the Taliban of Afghanistan, in so far as it concerns Mr Kadi and the Al Barakaat International Foundation.*

<sup>1469</sup> *Al-Dulimi and Montana Management Inc. v Switzerland* (Application no. 5809/08) (Court (First Instance)), (26 November 2013).

<sup>1470</sup> *ibid* [131].

<sup>1471</sup> *ibid*; Article 6(1). This was upheld by the Grand Chamber in 2016, in *Al-Dulimi and Montana Management Inc. v Switzerland* (Application no. 5809/08) (Court (Grand Chamber)), [2016] ECHR 576, whereby the Court found 15 to 2 in favour that Article 6(1) had been breached by the Swiss authorities.

<sup>1472</sup> Anderson D. *First Report on the Operation of the Terrorist-Asset Freezing etc. Act 2010* (HMSO, December 2011) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/223465/fin\\_sanc\\_report\\_on\\_terrorist\\_asset\\_freezing\\_151211.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/223465/fin_sanc_report_on_terrorist_asset_freezing_151211.pdf)> accessed June 2018; Terrorism (United Nations Measures) Order 2006 SI 2006/2657, Article 4(2).

<sup>1473</sup> Terrorist Asset Freezing etc. Act 2010 s. 2(1)(a)(i); *ibid* Anderson D.

expectations that the Terrorist Asset Freezing etc. Act is more in line with existing human rights legislation than the previous 2006 Orders. Moreover, as a current member of the European Union, UK legislation must now conform with EU asset freezing measures contained within Directive 2014/42/EU,<sup>1474</sup> which explicitly states that, due to its effects on human rights, there should be specific safeguards and judicial remedies,<sup>1475</sup> and freezing orders should be communicated to the affected person as soon as possible.<sup>1476</sup> Hence, the asset-freezing regime has become more robust, with a focus on the appropriateness of asset-freezing orders.

Yet despite the potential robustness of the asset-freezing regime, the Charity Commission and the Government has come under further scrutiny about the appropriateness of their actions towards charities since the Act, with concerns being raised by Muslim charities, who, like those in the US, believe that they have been unfairly targeted, because of the focus of both the Treasury and the Charity Commission on their work. For example, in 2014, the Muslim Charities Forum, which is an umbrella organisation for 10 Muslim charities including Islamic Relief and Muslim Aid, were informed that some of its members had links to terrorism,<sup>1477</sup> and was stripped of Government funding in 2015,<sup>1478</sup> which was intended to foster further integration within

---

<sup>1474</sup> Directive 2014/42/EU (3 April 2014) on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union.

<sup>1475</sup> *ibid* under Article 8. For example, Article 8(1) requires a right to an effective remedy and a fair trial and Article 8(2) requires effective communication of a freezing order as soon as possible after its execution.

<sup>1476</sup> *ibid* para. 33.

<sup>1477</sup> Turner, C. (The Telegraph, 23 September 2014) *Government donation to Muslim Charities Forum denounced as "madness"* <<http://www.telegraph.co.uk/news/uknews/11114599/Government-donation-to-Muslim-Charities-Forum-denounced-as-madness.html>> accessed November 2016, which highlighted that some of the charity's members had links to the Muslim Brotherhood through the Union of Good, which is a fundraising body for the Muslim Brotherhood. Muslim Hands, Human Appeal International, Human Relief Foundation, Muslim Aid and Islamic Relief were all alleged to have been early participants in the Union of Good.

<sup>1478</sup> Ross, T. (The Telegraph, 11 January 2015) *Muslim charity stripped of state funding over extremism fears* <<http://www.telegraph.co.uk/news/politics/conservative/11337846/Muslim-charity-stripped-of-state-funding-over-extremism-fears.html>> accessed November 2016; Pickles, E. (former Secretary of State for Communities and Local Government) *Written Statement: Integration Update*

the Muslim community.<sup>1479</sup> It was further found that over a quarter of statutory inquiries into charities by the Charity Commission were into Muslim charities which provided humanitarian relief or aid efforts in Syria between 2012 and 2014<sup>1480</sup> and that several financial institutions had blocked or delayed funds to or transfers from the accounts of Muslim and non-Muslim charities working in the Middle East.<sup>1481</sup> As noted by the Overseas Development, s. 17 of the 2010 Terrorist Asset Act provided the framework of granting licences “*to undertake actions related to making funds, financial services or economic resources available to or for the benefit of designated persons*”,<sup>1482</sup> which would be of assistance to humanitarian aid charities. However, the Overseas Development Institute (ODI) found that, although the potential for licences had been included in the Act, the Government had not provided guidance to charities and NGOs working in high risk zones to apply.<sup>1483</sup> During its research, the ODI also found that several charities, including Islamic Relief Worldwide, discovered the blocking of donations by UBS of their accountholders in 2012 and in 2014, the

---

HCWS154 (Hansard, 18 December 2014) <<http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2014-12-18/HCWS154/>> accessed November 2016.

<sup>1479</sup> Delmar-Morgan, A. (The Guardian, 22 July 2015) *Islamic charities in UK fear they are being unfairly targeted over extremism* <[https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share\\_btn\\_link](https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share_btn_link)> accessed November 2016.

<sup>1480</sup> *ibid*; from a Freedom of Information Request by The Guardian in 2014. Ramesh, R. (The Guardian, 16 November 2014) *Quarter of Charity Commission inquiries target Muslim groups* <<https://www.theguardian.com/society/2014/nov/16/charity-commission-inquiries-muslim-groups>> accessed November 2016.

<sup>1481</sup> *ibid*; In 2015, the Overseas Development Institute found that several leading financial institutions, such as HSBC, UBS and Natwest, had frozen the accounts of British charities working in Gaza, Syria and Iraq; Overseas Development Institute *UK humanitarian aid in the age of counterterrorism: perceptions and reality* (March 2015) <<https://www.odi.org/publications/9301-counter-terrorism-legislation-law-uk-muslim-ngos-charities-commission-humanitarian>> accessed November 2016; Arnold, M. (Financial Times, 4 March 2015) *Finance Denied to Charities in Conflict Zones, Report Finds* <<https://www.ft.com/content/540bdd9e-c299-11e4-a59c-00144feab7de>> accessed November 2016.

<sup>1482</sup> Overseas Development Institute *UK humanitarian aid in the age of counterterrorism: perceptions and reality* (March 2015) <<https://www.odi.org/publications/9301-counter-terrorism-legislation-law-uk-muslim-ngos-charities-commission-humanitarian>> accessed November 2016.

<sup>1483</sup> *ibid*.

Ummah Welfare Trust was told by HSBC that their account was to be closed.<sup>1484</sup> Finally, as part of their interviews, they were informed by another NGO that it had foregone £2million in donations during the previous 12 months because financial institutions had blocked their funds.<sup>1485</sup> Furthermore, Muslim charities note that there has been reputational damage caused by multiple investigations by the Charity Commission and the UK Government’s policy on extremism,<sup>1486</sup> in comparison with other charities such as the Red Cross, potentially causing Muslim charities and communities to be suspected without evidence of links to terrorism.<sup>1487</sup> The ‘Safer Giving’ campaign, targeted at UK Muslims who are giving to charity during the religious observance of Ramadan,<sup>1488</sup> has been particularly highlighted as an undue focus on charitable links with terrorist financing, creating a further schism between the Islamic community and those of other faiths.<sup>1489</sup> Clearly, a balance must be struck between monitoring those charities which are at risk from abuse from terrorist organisations and not focusing on a particular community, which risks further alienation and potential extremism.

Despite these concerns, the Act requires the appointment of an Independent Reviewer on asset-freezing orders, who would review the orders every twelve months,<sup>1490</sup> again allowing for more appropriate measures to be introduced should

---

<sup>1484</sup> *ibid.*

<sup>1485</sup> *ibid.*

<sup>1486</sup> E.g. Muslim Aid see Overseas Development Institute *UK humanitarian aid in the age of counterterrorism: perceptions and reality* (March 2015) <<https://www.odi.org/publications/9301-counter-terrorism-legislation-law-uk-muslim-ngos-charities-commission-humanitarian>> accessed November 2016.

<sup>1487</sup> *ibid*; Overseas Development Institute; Delmar-Morgan, A. (The Guardian, 22 July 2015) *Islamic charities in UK fear they are being unfairly targeted over extremism* <[https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share\\_btn\\_link](https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share_btn_link)> accessed November 2016.

<sup>1488</sup> Charity Commission *Safer Giving* <<https://www.gov.uk/government/news/ramadan-safer-giving>> accessed November 2016. This includes “Top 10 Tips” on safer giving during Ramadan.

<sup>1489</sup> *ibid* Delmar-Morgan, A.

<sup>1490</sup> Terrorist Asset Freezing etc. Act 2010, s. 31.

charities be unfairly targeted. As noted by the Independent Reviewer in 2011, however, the asset freezing regime after the passing of this Act became more ancillary in the fight against terrorist financing, as evidenced by the small amounts frozen – approximately £100,000 in the years 2010-2011 – the absence of those connected with Northern Irish terrorism, as well as the fact that many of the individuals and organisations designated had not been updated since 2001.<sup>1491</sup> While the appropriateness of this Act may have increased, the overall effectiveness of the asset freezing regime appears to have been in decline, as since 2008 the number of persons designated by HM Treasury has decreased,<sup>1492</sup> falling to 33 in 2014.<sup>1493</sup> Of these 33, eight were entities, and all of which had been on the list since 2001<sup>1494</sup> and the total amount frozen by HM Treasury was just £50,000 in 49 bank accounts by September 2014.<sup>1495</sup> With UK-linked individuals who have travelled to Syria fighting for the terrorist group ISIL<sup>1496</sup> and with ISIL finances estimated to run at approximately \$56million a month in 2016,<sup>1497</sup> it is difficult to see why the asset-freezing regime should further become

---

<sup>1491</sup> Anderson D. *First Report on the Operation of the Terrorist Asset Freezing etc. Act 2010*, (HMSO, December 2011), 14 <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/223465/fin\\_sanc\\_report\\_on\\_terrorist\\_asset\\_freezing\\_151211.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/223465/fin_sanc_report_on_terrorist_asset_freezing_151211.pdf)> accessed June 2018.

<sup>1492</sup> From 162 orders in 2008 to 38 in 2010-11 - see Anderson D. *Fourth Report on the Operation of the Terrorist Asset Freezing etc. Act 2010* (HMSO, March 2015), 9 <<https://www.gov.uk/government/publications/terrorism-and-terrorist-financing-fourth-independent-reviewer-report>> accessed November 2016.

<sup>1493</sup> *ibid.*

<sup>1494</sup> *ibid.*; of the entities included, four had links to Palestine or Lebanon, three are South American and one is Basque. The six Northern Irish entities were allowed to lapse in 2010, including the Real IRA and Continuity IRA, 11, para 2.21.

<sup>1495</sup> *ibid.* 11.

<sup>1496</sup> Thornberry, T. (Rt. Hon. Member for South Islington and Finsbury) *Written Question 40358* (Hansard, 27 June 2016)

<<https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-06-13/40358>> accessed November 2016. The Home Office estimated that out of this number, half had returned and a further 15% had been killed.

<sup>1497</sup> The seizure of 160 flash drives after an arrest of one of IS's operatives in Iraq in 2014 showed that IS's assets ran to \$2billion; Chulov, M. (The Guardian, 15 June 2014) *How an arrest in Iraq revealed Isis's \$2bn jihadist network*, <<https://www.theguardian.com/world/2014/jun/15/iraq-isis-arrest-jihadists-wealth-power>> accessed November 2016. The figure of \$56million a month was estimated in April 2016, is a reduction of 30% from the previous year, due to coalition airstrikes on Syrian oil-fields controlled by Islamic State and a lower tax collection; Reuters (18 April 2016) *Islamic State's*

ancillary to finding and disrupting terrorist financing, especially regarding Internet charities. Anderson added, due to the limited use of these powers, considering ISIL's presence in Syria and that many jihadists would require funding to travel to and from the conflict zones, as well as prepare for terrorist acts, that "[t]here is a case for more extensive use of TAFE 2010...".<sup>1498</sup> With these pressing concerns in mind, the UK's authorities must be able to swing the balance back towards effectiveness, while being mindful of the legal constraints they must adhere to, as well as the focus they have on certain international charities and the effects that over-restrictiveness of asset-freezing measures can have on genuine humanitarian causes.

### 5.3.2. Financial Institutions

The UK's approach to online banking and terrorist financing was much the same as the US in the aftermath of 9/11. For example, the UK adopted a more vigorous approach to its SAR regime for transactions over £10,000, and disclosure requirements, as the ATCSA inserted two new sections into the Terrorism Act 2000,<sup>1499</sup> making failure to disclose information about knowledge or suspicion of terrorism or crime under s. 15-18 an offence. Furthermore, the Proceeds of Crime Act 2002 dealt with the associated offence of money laundering, outlining penalties of up to five years and/or a

---

*income drops 30 per cent on lower oil, tax revenue* <<http://www.reuters.com/article/us-mideast-crisis-iraq-syria-islamic-sta-idUSKCN0XF0D5>> accessed November 2016; IHS Markit *Islamic State Monthly Revenue Drops to \$56 million, IHS Says* (18 April 2016) <<http://press.ihs.com/press-release/aerospace-defense-security/islamic-state-monthly-revenue-drops-56-million-ihs-says>> accessed November 2016.

NB. The increasing likelihood that Iraq's second city Mosul and its oilfields will be taken back by Iraqi forces will inevitably reduce IS's finances further.

<sup>1498</sup> Anderson D. *First Report on the Operation of the Terrorist Asset Freezing etc. Act 2010* (HMSO, December 2011), 19 <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/223465/fin\\_sanc\\_report\\_on\\_terrorist\\_asset\\_freezing\\_151211.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/223465/fin_sanc_report_on_terrorist_asset_freezing_151211.pdf)> accessed June 2018.

<sup>1499</sup> Terrorism Act 2000 c.11, s. 21A, s. 21B.



fine for financial institutions to fail to disclose suspicions of money laundering.<sup>1500</sup> As with the US, this has increased the burden upon the regulated sector and financial intelligence units (FIUs) to locate and file SARs which may reveal the transfer of terrorist finances.<sup>1501</sup> During 2014-15, 381,882 were filed with the National Crime Agency (NCA)<sup>1502</sup> compared with less than 20,000 in 2000.<sup>1503</sup> It was further found by the NCA that over 83% of these SARs were filed by the banking sector,<sup>1504</sup> compared with only 2.91% from Money Services Businesses.<sup>1505</sup> Of the SARs filed in 2014-15, just 1,899 were referred to the National Terrorist Financial Investigation Unit and the Counter Terrorism Unit.<sup>1506</sup> As noted in chapter four, the sheer number of SARs can make searching for a potential link to terrorism more difficult to find. As also highlighted with the US, the general “know your customer” rules imposed upon financial institutions become less effective in non-face-to-face transactions such as electronic banking, due to the lack of supporting documentation and physical presence.<sup>1507</sup> Despite these concerns, in December 2007, the UK implemented the European Union’s Third Money Laundering Directive<sup>1508</sup> through the Money Laundering

---

<sup>1500</sup> Part 7 Proceeds of Crime Act 2002 c.29, s. 330 (failure to disclose: regulated sector), s. 334 (penalties).

<sup>1501</sup> See in general regarding criticisms of SARs, Ryder, N. *A False Sense of Security? An analysis of Legislative Approaches Towards to Prevention of Terrorist Finance in the United States and the United Kingdom* (2007) J.B.L. Nov 821, 836 (US); 846-8 (UK).

<sup>1502</sup> National Crime Agency *Suspicious Activity Reports (SARs) Annual Review 2015*, 6 <[www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015](http://www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015)>, accessed November 2016.

<sup>1503</sup> Lander, S. *Review of the Suspicious Activity Reports Regime* (London: SOCA, March 2006), 13.

<sup>1504</sup> *ibid* National Crime Agency *Suspicious Activity Reports (SARs) Annual Review 2015*, 9.

<sup>1505</sup> *ibid*. ‘Money Services Businesses’ include those businesses which “transmit money or any representation of money, in any way” under the Money Laundering Regulations 2007 SI 2007/2157; HM Revenue & Customs *Money Laundering Regulations: Money Service Business registration* (February 2014) <<https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration>> accessed November 2016, and must be registered under s.26. This would include the *hawala* system of informal value transfer, and will be expanded upon in Chapter six.

<sup>1506</sup> *ibid* 31.

<sup>1507</sup> Basel Committee on Banking Supervision *Customer Due Diligence for Banks* (October 2001) 11, paras. 45-48 <<http://www.bis.org/publ/bcbs85.pdf>> accessed November 2016.

<sup>1508</sup> Directive 2005/60/EC (26 October 2005) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (“Third Money Laundering Directive”).

Regulations 2007 (MLR). Again, there is focus on Customer Due Diligence measures,<sup>1509</sup> placing the onus on financial institutions to identify customers which are not physically present,<sup>1510</sup> including extra documentation<sup>1511</sup> and subsequent contact with the potential customer.<sup>1512</sup> As Donohue highlights, such measures can be counteractive, the “*white noise created by the deluge of data increas[ing] the difficulty of ferreting out real threats*”.<sup>1513</sup> Consequently, the UK suffers from over-regulation in this area, as with an estimated 60% of all adult Internet users using online banking,<sup>1514</sup> the problem of tracing terrorist financing is again evident when combined with SARs from online banking.<sup>1515</sup>

This difficulty is made even more impossible when financial institutions themselves have enabled terrorist financing. In 2012, the US Senate Committee found that HSBC a British-based financial institutions, with its subsidiary banks, HBUS and HSMX, had colluded in money laundering with Mexican cartels, as well as terrorist financing with affiliates in Iran and the Middle East.<sup>1516</sup> The report found that HBUS

---

NB. The UK Government is about to transpose the Fourth Money Laundering Directive into law; HM Treasury *Transposition of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016.

<sup>1509</sup> Money Laundering Regulations 2007 SI 2007/2157, Part 2 s. 5-18.

<sup>1510</sup> *ibid* s. 14(2).

<sup>1511</sup> Money Laundering Regulations 2007 SI 2007/2157, s. 14(2)(a).

<sup>1512</sup> *ibid* s. 14(2)(b).

<sup>1513</sup> Donohue, L. K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int'l L 303, 395.

<sup>1514</sup> Office of National Statistics *Internet access – households and individuals: 2016* (4 August 2016) <<http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetand-socialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016>> accessed November 2016.

<sup>1515</sup> Money Laundering Regulations 2007 SI 2007/2157, s. 5-18; there is customer due diligence for financial institutions to insist upon customer ID when they are not present. However, as Donohue argues, this can be counter-productive; Donohue, L. K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int'l L 303, 395.

<sup>1516</sup> US Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations *HSBC Exposed U.S. Financial System to Money Laundering, Drug, Terrorist Financing Risks* (16 July 2012) <<https://www.hsgac.senate.gov/subcommittees/investigations/media/hsbc-exposed-us-financial-system-to-money-laundering-drug-terrorist-financing-risks>> accessed November 2016.

had circumvented rules preventing them from dealing with states subject to US sanctions at the time, such as North Korea, Iran and Burma,<sup>1517</sup> carrying out 28,000 sensitive and undisclosed transactions between 2001 and 2007, including \$19.4bn of transactions to Iran,<sup>1518</sup> and that HSBC Europe and HSBC Middle East had altered this transaction information to delete any reference to Iran.<sup>1519</sup> Furthermore, HSBC had worked with Al Rajhi Bank, which was alleged to have links to terrorist financing after 9/11,<sup>1520</sup> resuming links with the bank in 2006, despite internal concerns about the risk and a severing of ties in 2005.<sup>1521</sup> Finally, the Report found that there had been a large backlog of SARs at the bank, which contributed to the missing of important information.<sup>1522</sup> Thus, due to these severe internal failings of HSBC, the SARs regime appears almost redundant, and bank reporting systems need to be strengthened to prevent abuse. Another troubling result of the HSBC findings is the fact that, while the US fined the bank \$1.9billion in 2012,<sup>1523</sup> the UK failed to follow suit. In July 2016,

---

<sup>1517</sup> US Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations *U.S. Vulnerabilities to Money Laundering, Drugs and Terrorist Financing: HSBC Case History* (17 July 2012), 114 <<http://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history>> accessed November 2016.

<sup>1518</sup> *ibid* 113. The Report notes that: “To ensure HBUS cleared the transactions without delay, HBEU routinely altered transaction documentation to delete any reference to Iran that might trigger the OFAC filter at HBUS and also typically characterized the transaction as a transfer between banks in permitted jurisdictions”.

<sup>1519</sup> Simpson, G.R. (Wall Street Journal, 26 July 2007) *U.S. Tracks Saudi Bank Favored by Extremists* <<http://www.wsj.com/articles/SB118530038250476405>> accessed November 2016, which highlighted the concerns by the CIA about the bank’s transactions in 2003; the Senate Committee Report also notes this, 197-198; the Report notes the links of the bank to a number of accounts held by the disgraced al-Haramain Islamic Foundation, which was found to have had direct links with al-Qa’eda, 199-200. Furthermore, families of the victims of 9/11 have attempted to sue Al Rajhi Bank for providing material support for 9/11, but failed in 2005 to win their case before the District Court. In 2014, the Supreme Court had declined to consider the case. See *John Patrick O’Neill et al. v. Al Rajhi Bank et al.* [2014] United States Supreme Court No. 13-318.

<sup>1520</sup> US Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations *U.S. Vulnerabilities to Money Laundering, Drugs and Terrorist Financing: HSBC Case History* (17 July 2012), 189-224 <<http://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history>> accessed November 2016.

<sup>1521</sup> *ibid* 203-204; 206-220.

<sup>1522</sup> *ibid* 30-32.

<sup>1523</sup> BBC News (11 December 2012) *HSBC to pay \$1.9bn in US money laundering penalties* <<http://www.bbc.co.uk/news/business-20673466>> accessed November 2016.

it was revealed by a US Committee on Financial Services Congressional Report that the former UK Chancellor of the Exchequer, George Osborne, had asked for criminal charges to be dropped against HSBC in 2012, “*warning of possible financial calamity if DOJ [Department of Justice] were to prosecute HSBC*”.<sup>1524</sup> Clearly, while the issue of financial stability was at stake for the UK Government so soon after the financial crash of 2008, the precedent this decision sets is troubling. Without formal financial institutions’ co-operation or accession to the legal framework of the countries they carry out their business in, the reliability of the SARs regime is at risk through purposeful collusion, as happened with HSBC. By failing to ensure that HSBC was set as an example to other financial institutions to ensure their reporting mechanisms are not open to abuse, the UK Government has placed the SARs reporting scheme through formal financial institutions in danger of becoming ineffective.

Additionally, the problem of tracing terrorist financing through SARs was also no more apparent than in the wake of the London bombings on 7 July 2005. Although the subsequent Lander Review in 2005 and the Serious Organised Crimes Act 2005 addressed the problem of the SARs regime and detecting terrorist financing, for example, centralising investigations to one agency, the Serious Organised Crimes Agency,<sup>1525</sup> and identifying weaknesses in the system,<sup>1526</sup> the 7/7 bombings opened up a new aspect of terrorist financing - the low cost of organising terrorist acts. As

---

<sup>1524</sup> US House of Representatives Financial Services Committee *Too Big to Jail: Inside the Obama Justice Department’s Decision not to hold Wall Street Accountable* (11 July 2016) <[financialservices.house.gov/uploadedfiles/07072016\\_oi\\_tbtj\\_sr.pdf](http://financialservices.house.gov/uploadedfiles/07072016_oi_tbtj_sr.pdf)> accessed November 2016; Neate, R. (The Guardian, 11 July 2016) *HSBC escaped US money-laundering charges after Osborne’s intervention* <<https://www.theguardian.com/business/2016/jul/11/hsbc-us-money-laundering-george-osborne-report>> accessed November 2016.

<sup>1525</sup> *ibid* Lander, S. *Review of the Suspicious Activity Reports Regime* (London: SOCA, March 2006), 19.

<sup>1526</sup> *ibid* 26.

Cliff Knuckey, a former Metropolitan Police Detective Inspector and Operations Director of RISC Management stated in May 2006, “...*The March [2004] Madrid bombings were carried out at a cost of less than \$7,000 USD... the 7/7 bombings in London last year were carried out for less than \$1,000 USD...*”.<sup>1527</sup> In the subsequent Report on 7/7, it was estimated that the bombings cost a total of £8,000, including training trips and organisation,<sup>1528</sup> below the £10,000 limit for financial institutions to automatically submit SARs. The Report further noted that the group “*appears to have raised the necessary cash by methods that would be extremely difficult to identify as related to terrorism or other serious criminality*”.<sup>1529</sup> As outlined with the US, such funds raised would not raise suspicion and remain undetected in the formal financial system.<sup>1530</sup> This has again been highlighted by subsequent terrorist attacks in both the US and the UK since 9/11 – for example, the Boston Marathon attacks killing 5 were carried out with homemade pressure cookers for less than \$100<sup>1531</sup> and the death of

---

<sup>1527</sup> Knuckey, C., quoted in <[http://www.gsnmagazine.com/may\\_06/terrorists\\_funds.html](http://www.gsnmagazine.com/may_06/terrorists_funds.html)> accessed November 2016; Ryder, N. *A False Sense of Security? An analysis of Legislative Approaches Towards to Prevention of Terrorist Finance in the United States and the United Kingdom* (2007) J.B.L. Nov 821, 848.

<sup>1528</sup> Home Office *Report of the Official Account of the Bombings in London on 7th July 2005* HC1087 (HMSO, 11 May 2006), 23 <<https://www.gov.uk/government/publications/report-of-the-official-account-of-the-bombings-in-london-on-7th-july-2005>> accessed November 2016. From the Report, it was clear that Siddique Khan had provided most of the financing himself – “*Having been in full-time employment for 3 years since University, he had a reasonable credit rating, multiple bank accounts (each with just a small sum deposited for a protracted period), credit cards and a £10,000 personal loan.*”; *ibid.*

<sup>1529</sup> *ibid.*

<sup>1530</sup> Donohue, L.K. *Anti Terrorist Finance in the United Kingdom and the United States* (2005-2006) 27 Michigan Journal of International Law 303, 432; FIPR Report on Privacy, 25 ref MasterCard daily transactions.

<sup>1531</sup> The components for the bombs were low cost – consisting of pressure cookers, BB pellets and nails, which are available at most stores. Warrick, J. & Horwitz, S. (Washington Post, 16 April 2013) *Boston Marathon bombs had simple but harmful design, early clues indicate* <[https://www.washingtonpost.com/world/national-security/boston-marathon-bombs-had-simple-but-harmful-design-early-clues-indicate/2013/04/16/c2b061cc-a6d8-11e2-8302-3c7e0ea97057\\_story.html](https://www.washingtonpost.com/world/national-security/boston-marathon-bombs-had-simple-but-harmful-design-early-clues-indicate/2013/04/16/c2b061cc-a6d8-11e2-8302-3c7e0ea97057_story.html)> accessed November 2016; *United States v Dzhokhar A. Tsarnaev* District of Massachusetts Case Number: 13-cr-10200. Tsarnaev was sentenced to death in 2015; Department of Justice District Attorney’s Office District of Massachusetts *Judge Imposes Death Sentence for Boston Marathon Bomber* (24 June 2015) <<https://www.justice.gov/usao-ma/pr/judge-imposes-death-sentence-boston-marathon-bomber>> accessed November 2016.

Lee Rigby in Woolwich in 2013 was carried out with machetes,<sup>1532</sup> which can cost as little as £7.99 online.<sup>1533</sup> Compared with the \$333million it cost the Boston economy in the wake of the Boston bombings,<sup>1534</sup> all the above cases highlight the wider damage caused by cheap terrorism, which essentially hampers law enforcement authorities from being able to carry out the aims of the 1999 Convention.<sup>1535</sup> Thus, there has been concern about the effectiveness of the SARs regime in the wake of the 7/7 bombings.

However, the UK Government's efforts to combat 'cheap' terrorism since then has been to implement the Prevent strand of the CONTEST counter-terrorism strategy,<sup>1536</sup> which aims to prevent people from being drawn into terrorism.<sup>1537</sup> The US has a similar scheme, the Countering Violent Extremism Programme,<sup>1538</sup> which administers grants and provides support – but does not go as far as Prevent.<sup>1539</sup> After the

---

<sup>1532</sup> *R v Adebolajo and another* [2014] All ER (D) 37.

<sup>1533</sup> On a broad Google search, there are a wide variety of large machetes and knives available at low cost; the one referenced is an 18" Bushcraft Survival Machete at £7.99 at Springfields <https://www.springfields.co.uk/18-bushcraft-survival-machete.html> accessed November 2016

<sup>1534</sup> Dedman, B. & Schoen, J. (NBC News, 30 April 2013) *Adding up the financial costs of the Boston bombings* <[http://usnews.nbcnews.com/\\_news/2013/04/30/17975443-adding-up-the-financial-costs-of-the-boston-bombings](http://usnews.nbcnews.com/_news/2013/04/30/17975443-adding-up-the-financial-costs-of-the-boston-bombings)> accessed November 2016.

<sup>1535</sup> Chapter one, 1.4.2.1.

<sup>1536</sup> NB. CONTEST was updated in 2011. CONTEST has four strands; Home Office *CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2015* Cm9310 (26 July 2016) <<https://www.gov.uk/government/publications/contest-uk-strategy-for-countering-terrorism-annual-report-for-2015>> accessed November 2016.

<sup>1537</sup> Prevent has three objectives – (i) respond to the ideological challenge of terrorism and the threat faced from those who promote it; (ii) prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support; and (iii) work with sectors and institutions where there are risks of radicalisation which need to be addressed; HM Government *Prevent Strategy* <[https://www.gov.uk/government/uploads/system/uploads/attachmentatachment/136226/prevent\\_strategy\\_review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachmentatachment/136226/prevent_strategy_review.pdf)> accessed November 2016.

<sup>1538</sup> Department for Homeland Security *Countering Violent Extremism* <<https://www.dhs.gov/countering-violent-extremism>> accessed November 2016.

<sup>1539</sup> *ibid* The Office for Community Partnerships provides assistance and support among the following streams for communities: (a) Community Engagement to build awareness and promote dialogue; (b) Field Support Expansion and Training to support Department for Homeland Security field staff; (c) Grant support through the Federal Emergency Management Agency to issue a notice of funding opportunities (d) Philanthropic Engagement, to maximise support for local communities and (e) Tech Sector Engagement, 'to identify and amplify credible voices online and promote counter narratives against violent extremist messaging'.

7/7 bombings, the Terrorism Act 2006 was introduced, making it an offence to encourage terrorism<sup>1540</sup> as well as to disseminate terrorist publications,<sup>1541</sup> extending its application to use over the Internet.<sup>1542</sup> As such, the Act created a far-reaching offence, which blurs the line between freedom of speech, extremism, and terrorism. To separate out the differences between extremism and terrorism, Prevent also works with several sector bodies, including education, faith, health, criminal justice and charities<sup>1543</sup> to carry out its aims, and uses the Terrorism Act 2006 to distinguish between extremist and terrorist language.<sup>1544</sup> Of the early findings of Prevent, it was shown that in 2007/8, 261 projects delivered in England in 2007/08 had reached an estimated 44,000 people,<sup>1545</sup> potentially becoming an effective tool to combat cheap terrorism. Furthermore, cases such as Andrew ‘Isa’ Ibrahim in 2009, who was turned into law enforcement authorities by his community before he attempted to set off a bomb,<sup>1546</sup> and despite missed opportunities by local businesses and the City of Bristol College<sup>1547</sup> shows that Prevent had potentially an effective side to it.<sup>1548</sup> Nevertheless, despite

---

<sup>1540</sup> Terrorism Act 2006 c.11, s. 1(2).

<sup>1541</sup> Terrorism Act 2006 c.11, s. 2.

<sup>1542</sup> Terrorism Act 2006 c.11, s. 3.

<sup>1543</sup> *ibid.*

<sup>1544</sup> *ibid.*

<sup>1545</sup> *ibid* *Prevent Strategy Review* <<https://www.gov.uk/government/uploads/system/.../prevent-strategy-review.pdf>> accessed November 2016.

<sup>1546</sup> Gardham, D. (The Telegraph, 18 July 2009) *Terrorist Andrew Ibrahim was turned in by the Muslim community* <<http://www.telegraph.co.uk/news/5851168/Terrorist-Andrew-Ibrahim-was-turned-in-by-the-Muslim-community.html>> accessed November 2016.

<sup>1547</sup> *ibid.*

<sup>1548</sup> Furthermore, the missed opportunities by public sector services were clear in several other cases – for instance, Nicky Reilly (Mohamed Saeed-Alim), this was missed by the NHS who had contact with him through mental health services, as he had Asperger’s as well as learning difficulties (he later killed himself in prison); The Telegraph (21 October 2016) *Muslim convert who partially blew himself up in a Giraffe restaurant in a failed suicide attack found dead in prison* <<http://www.telegraph.co.uk/news/2016/10/21/muslim-convert-who-blew-up-restaurant-with-nail-bomb-fo/>> accessed November 2016; also Taimour Abdulwahab al-Abdaly, who had been expelled from a mosque in Luton for his extremist views (but did not refer him to authorities), yet later killed himself in a bomb attack in Stockholm; Jones, S. & Siddique, H. (The Guardian, 13 December 2010) *Stockholm suicide bomber confronted by Luton mosque leaders* <<https://www.theguardian.com/world/2010/dec/13/stockholm-suicide-bomber-luton-mosque>> accessed November 2016; *ibid* *Prevent Strategy Review*, 56.

funding community projects, it was found that some of central Government finances had been channelled into extremist causes,<sup>1549</sup> thereby limiting its effectiveness. A Review of Prevent in 2011 highlighted that “[r]ecords and audit trails for Prevent funding have not always been comprehensive. It is therefore possible that Prevent funding has reached extremist groups...”,<sup>1550</sup> showing that funding for anti-radicalisation programmes was not being properly audited, and potentially found its way towards extremist groups. Despite refocusing the Prevent Strategy since this Review, in 2015, a 15-year old boy, who was referred to the Channel programme under the Prevent scheme,<sup>1551</sup> was sentenced to life in prison with a minimum sentence of five years, for inciting terrorism overseas.<sup>1552</sup> The schoolboy had exchanged over 3,000 encrypted social media messages with Sevdet Besim, a Melbourne-based man, and encouraged him to carry out a terrorist attack on Anzac Day in Australia.<sup>1553</sup> Indeed, the presiding judge, Mr Justice Saunders, stated that the child had been referred to Channel by his school in 2013, but had only paid “lip service” to the programme<sup>1554</sup>

---

<sup>1549</sup> Rt Hon. Theresa May MP, former Home Secretary, stated “[i]n trying to reach out to those at risk of radicalisation, funding sometimes even reached the very extremist organisations that Prevent should have been confronting.” May, T. *Oral Statement* (Hansard, 8 June 2011) <<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110607/debtext/110607-0002.htm#11060740000001>> accessed November 2016; *ibid Prevent Strategy Review*, 32.

<sup>1550</sup> *ibid Prevent Strategy Review*, 35 para. 6.63 <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/44444/prevent-strategy-review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/44444/prevent-strategy-review.pdf)> accessed November 2016.

<sup>1551</sup> Channel is the application of the Prevent Strategy. Home Office *Channel Guidance* (2012) <<https://www.gov.uk/government/publications/channel-guidance>> accessed November 2016.

<sup>1552</sup> He was the youngest ever to be prosecuted and jailed for terrorism offences in the UK and was reported to authorities on 25 March 2015 by his school due to his behaviour, which resulted in classmates nicknaming him ‘The Terrorist’; Crown Prosecution Service *15 year old jailed for part in international terror plot* (2 October 2015)

<[http://www.cps.gov.uk/news/latest\\_news/15\\_year\\_old\\_jailed\\_for\\_part\\_in\\_international\\_terror\\_plot/](http://www.cps.gov.uk/news/latest_news/15_year_old_jailed_for_part_in_international_terror_plot/)> accessed November 2016; Elgot, J. (The Guardian, 2 October 2015) *UK schoolboy given life sentence for Australia terror plot* <<https://www.theguardian.com/world/2015/oct/02/uk-school-boy-life-sentence-australia-terror-plot>> accessed November 2016.

<sup>1553</sup> NB. Anzac Day commemorates the Australian losses at Gallipoli during the First World War. Sevdet Besim planned to run over and behead a police officer (similar to Woolwich in 2013) and, more outlandishly, fill a kangaroo with explosives on Anzac Day, *ibid*; Elgot J., Osborne S. (The Independent 5 September 2016) *Australian teen Sevdet Besim jailed for Anzac Day terror plot* <<http://www.independent.co.uk/news/world/australasia/australian-teen-sevdet-ramadan-besim-jailed-anzac-day-terror-plot-melbourne-dandenong-a7226891.html>> accessed November 2016.

<sup>1554</sup> *ibid* Elgot, J.



and that “[h]e communicated with extremist propagandists who either worked for Isis or supported their aims over the internet,” who “were experienced recruiters who were keen to enlist young impressionable Muslims to the cause”.<sup>1555</sup>

This case clearly highlights that, there has been difficulty in reaching those most in need through the Prevent and Channel programmes who, like many young people, use social media. For example, al-Qaeda in the Arabian Peninsula’s INSPIRE magazine, which was launched in 2010,<sup>1556</sup> includes bomb-making instructions for bombs which could evade airport security<sup>1557</sup> and, in the issue released in September 2015, called on African Americans to convert to their cause,<sup>1558</sup> capitalising on racial tensions currently present within the US.<sup>1559</sup> Significantly, in several acts of terrorism, the issues of this magazine have been present. For example, issue one of INSPIRE had an article entitled “*How to Build a Bomb in your Mom’s Kitchen*”,<sup>1560</sup> with instructions on how to build a pressure cooker bomb cheaply (present in Boston), and another one of the magazine’s issues called for lone wolves to use vehicles run over

---

<sup>1555</sup> *ibid.*

<sup>1556</sup> This was said to have been the work of Anwar al-Awlaki, before his death in 2011. Finn, P. (Washington Post, 2 May 2012) *Inspire, al-Qaeda’s English-language magazine, returns without editor Awlaki* <[https://www.washingtonpost.com/world/national-security/inspire-al-qaedas-english-language-magazine-returns-without-editor-awlaki/2012/05/02/gIQAiEPMxT\\_story.html](https://www.washingtonpost.com/world/national-security/inspire-al-qaedas-english-language-magazine-returns-without-editor-awlaki/2012/05/02/gIQAiEPMxT_story.html)> accessed November 2016; Lieberman, J. I., (Chairman) & Collins, Susan M. (Ranking Member) *A Ticking Time Bomb: Counter-terrorism Lessons from the US Government’s Failure to Prevent the Fort Hood Attack* 20510 (U.S. Senate Committee on Homeland Security and Governmental Affairs Washington D.C. February 2011) <[www.hsgac.senate.gov/public/files/Fort\\_Hood/FortHoodReport.pdf](http://www.hsgac.senate.gov/public/files/Fort_Hood/FortHoodReport.pdf)> accessed November 2016.

<sup>1557</sup> Anti-Defamation League *13th Issue of AQAP Inspire Calls for Attacks Against U.S. Airlines* (24 December 2014) <[http://blog.adl.org/extremism/aqap-al-qaeda-inspire-english-magazine-13?\\_ga=1.243425985.530138109.1478458603](http://blog.adl.org/extremism/aqap-al-qaeda-inspire-english-magazine-13?_ga=1.243425985.530138109.1478458603)> accessed November 2016.

<sup>1558</sup> Anti-Defamation League *New AQAP Inspire Magazine Encourages Lone Wolf Attacks* (21 September 2015) <[http://blog.adl.org/extremism/new-aqap-inspire-magazine-encourages-lone-wolf-attacks?\\_ga=1.54290028.530138109.1478458603](http://blog.adl.org/extremism/new-aqap-inspire-magazine-encourages-lone-wolf-attacks?_ga=1.54290028.530138109.1478458603)> accessed November 2016.

<sup>1559</sup> For example, the Black Lives Matter campaign; Ross, J. (Washington Post, 19 August 2015) *How Black Lives Matter moved from a hashtag to a real political force* <<https://www.washingtonpost.com/news/the-fix/wp/2015/08/19/how-black-lives-matter-moved-from-a-hashtag-to-a-real-political-force/>> accessed November 2016.

<sup>1560</sup> Spencer, R. (The Telegraph, 16 April 2013) *Boston Marathon bombs: al-Qaeda’s Inspire magazine taught pressure cooker bomb-making techniques* <<http://www.telegraph.co.uk/news/world-news/al-qaeda/9998886/Boston-Marathon-bombs-al-Qaedas-Inspire-magazine-taught-pressure-cooker-bomb-making-techniques.html>> accessed November 2016.

targets, as happened with Lee Rigby in Woolwich in 2013<sup>1561</sup> and later in Nice in 2016.<sup>1562</sup> Although possession of this magazine has been successfully prosecuted under s. 58 of the Terrorism Act 2000,<sup>1563</sup> it is still providing inspiration for others to potentially carry out terrorist acts and is still present on the Internet. Furthermore, the insidious nature of ISIL and its use of social media, as mentioned before, has caused approximately 850 British citizens to travel to Syria,<sup>1564</sup> including a number of vulnerable school children.<sup>1565</sup> Consequently, the territorial reach of Prevent is not far enough to counteract the issue of cheap terrorism and the all-encompassing nature of propaganda spread by terrorist groups over the Internet, thereby limiting its effectiveness.

---

<sup>1561</sup> Black, I. (The Guardian, 24 May 2013) *Inspire magazine: the self-help manual for al-Qaida terrorists* <<https://www.theguardian.com/world/shortcuts/2013/may/24/inspire-magazine-self-help-manual-al-qaida-terrorists>> accessed November 2016.

<sup>1562</sup> BBC News (19 August 2016) *Nice attack: What we know about the Bastille Day killings* <<http://www.bbc.co.uk/news/world-europe-36801671>> accessed November 2016.

<sup>1563</sup> For example, Mohammed Abul Hasnath and Ruksana Begum were both imprisoned for possessing copies of the magazine under s. 58 Terrorism Act 2000 c.11; BBC News (20 June 2012) *Mohammed Abdul Hasnath jailed for 14 months over terror charges* <<http://www.bbc.co.uk/news/uk-england-london-18528573>> accessed November 2016; BBC News (6 December 2012) *Al-Qaeda material bride Ruksana Begum jailed* <<http://www.bbc.co.uk/news/uk-england-london-20629275>> accessed November 2016.

<sup>1564</sup> Thornberry, T. (Rt. Hon. Member for South Islington and Finsbury) *Written Question 40358* (Hansard, 27 June 2016)

<<https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-06-13/40358>> accessed November 2016.

<sup>1565</sup> For example, Kadiza Sultana, who left her London home with two of her friends, Shamima Begum and Amira Abase in 2015, was recently feared dead in an airstrike in Syria. Henley J. and Dodd, V. (The Guardian, 12 August 2016) *Kadiza Sultana: London schoolgirl who joined Isis believed killed in Syria airstrike* <<https://www.theguardian.com/uk-news/2016/aug/11/london-school-girl-kadiza-sultana-who-joined-isis-believed-killed-in-syria-airstrike>> accessed November 2016; Zahra and Halma Halane, 17 year old twins, left Manchester for Syria in 2014; Spencer, R. (The Telegraph, 3 February 2015) *Target practice: Teenage British twins train in Syria* <<http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11387424/Target-practice-Teenage-British-twins-train-in-Syria.html>> accessed November 2016.

NB. Their cousin, Abdullahi Ahmed Jama Farah, was imprisoned for seven years after helping one of his friends travel to Syria and using his mother's house as a communications hub for the 'Brittani Brigade', for UK-based IS fighters: BBC News (11 February 2016) *Manchester student guilty of terror offences* <<http://www.bbc.co.uk/news/uk-england-manchester-35549985>> accessed November 2016; 21 year old Aqsa Mahmood left Glasgow in 2013, becoming prolific at spreading ISIL propaganda online; Dearden, L. (The Independent, 12 August 2016) *Isis' British brides: What we know about the girls and women still in Syria after the death of Kadiza Sultana* <<http://www.independent.co.uk/news/uk/home-news/isis-british-brides-kadiza-sultana-girls-women-syria-married-death-killed-aqsa-mahmood-islamic-state-a7187751.html>> accessed November 2016.

Additionally, Prevent has been severely criticised on many levels since it was introduced. For instance, as the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly,<sup>1566</sup> Maina Kiai, highlighted in 2016, by “*dividing, stigmatising and alienating segments of the population, Prevent could end up promoting extremism, rather than countering it.*”<sup>1567</sup> Although the Prevent Strategy purports to cover all forms of terrorism, including Islamist, Northern Irish, extreme far right and ‘other’ terrorist groups,<sup>1568</sup> there has been more of a focus on Islamic extremism since its inception. The Prevent Strategy is also explicit in its funding strategy, stating that “*the allocation of resources will be proportionate to the threats we face. At present the greatest threat to the UK as a whole is from Al Qa’ida and groups and individuals who share the violent Islamist ideology associated with it*”,<sup>1569</sup> meaning that the main focus of Prevent has been on radicalisation within Muslim communities. This is no more evident than through Prevent referral figures, which showed that, between 2007 and 2010, 67% of referrals involved Muslims<sup>1570</sup> and, between 2012 and 2014, 56%

---

<sup>1566</sup> This is mandated through the UN Human Rights Council Resolution A/HRC/RES/15/21 The rights to freedom of peaceful assembly and of association (10 June 2010), (5(c)), and submits annual reports to the UN Human Rights Council and General Assembly and carries out fact finding missions; United Nations *Human Rights Office of the High Commissioner* <<http://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/SRFreedomAssemblyAssociationIndex.aspx>> accessed November 2016.

<sup>1567</sup> Gayle, D. (The Guardian, 21 April 2016) *Prevent strategy 'could end up promoting extremism'* <<https://www.theguardian.com/politics/2016/apr/21/government-prevent-strategy-promoting-extremism-maina-kiai>> accessed November 2016.

<sup>1568</sup> Home Office, *Prevent Strategy*, (June 2011) 13-15 <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/101111/prevent-strategy-review.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/101111/prevent-strategy-review.pdf)> accessed November 2016.

<sup>1569</sup> *ibid Prevent Strategy*, 6, para. 3.12.

<sup>1570</sup> *ibid Prevent Strategy*, 60, para. 9.24.

of referrals involved Muslims,<sup>1571</sup> even though Muslims make up just 5% of the population in England and Wales.<sup>1572</sup> Additionally, 415 children under the age of 10 have been referred to Channel, the intervention service of Prevent since 2012,<sup>1573</sup> highlighting the significant reach and scope of the strategy and calling into question its appropriateness. Under the Counter-Terrorism and Security Act 2015, schools, higher education institutions and the NHS are now under a legal obligation to prevent people from being drawn to terrorism.<sup>1574</sup> Yet this has been applied through Prevent and Channel in a significantly broad manner by some education institutions. Several high-profile cases of over-zealous application of Prevent have further been evident in cases of nursery and school children - for example, it was discussed by a four-year old's nursery to refer him to the Channel programme for drawing a 'cooker bomb', when it depicted his father cutting up a cucumber,<sup>1575</sup> and a 14-year old Muslim schoolboy

---

<sup>1571</sup> National Police Chiefs' Council, *National channel referral figures* <<http://www.npcc.police.uk/FreedomofInformation/NationalChannelReferralFigures.aspx>> accessed November 2016. NB. This was a Freedom of Information request regarding the Channel referral service under the Prevent strategy; Halliday, J. (The Guardian, 20 March 2016) *Almost 4,000 people referred to UK deradicalisation scheme last year* <<https://www.theguardian.com/uk-news/2016/mar/20/almost-4000-people-were-referred-to-uk-deradicalisation-scheme-channel-last-year>> accessed November 2016. However, on reading the NPCC's figures, this author believes that the article was incorrect, as the 3934 people referred to organisations under Channel represent the total number between 2006 and 2014 and, in fact, 1281 people were referred in 2013/14. The figures do, however, show a large increase between 2012 and 2014 – from 748 to 1281.

<sup>1572</sup> This equates to roughly 2.7million and is compared with 59%, or 33.2million, who identified themselves as Christian in England and Wales; Office for National Statistics *2011 Census: Key Statistics for England and Wales, March 2011* (11 December 2012), 8 <<http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/stb-2011-census-key-statistics-for-england-and-wales.html>> accessed November 2016.

<sup>1573</sup> Kotecha, S. (BBC News, 21 January 2016) *More than 400 children under 10 referred for 'deradicalisation'* <<http://www.bbc.co.uk/news/uk-35360375>> accessed November 2016. This was a Freedom of Information request by the BBC, which also showed that over 1,800 children under the age of 15 were referred.

<sup>1574</sup> Counter-Terrorism and National Security Act 2015 c.6, s. 26(1).

<sup>1575</sup> Qunn, B. (The Guardian, 11 March 2016) *Nursery 'raised fears of radicalisation over boy's cucumber drawing'* <<https://www.theguardian.com/uk-news/2016/mar/11/nursery-radicalisation-fears-boys-cucumber-drawing-cooker-bomb>> accessed November 2016; BBC News (11 March 2016) *Radicalisation fear over cucumber drawing by boy, 4* <<http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-35783659>>; Barratt D. (The Telegraph, 11 March 2016) *Four-year-old who 'mispronounced the word cucumber' threatened with counter-terrorism measures* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12191543/Four-year-old-who-mispronounced-the-word-cucumber-threatened-with-counter-terrorism-measures.html>> accessed November 2016.

was questioned by his school for discussing ‘eco-terrorism’ in his classroom.<sup>1576</sup> Both cases have also shown a gap in the training available to teachers under Prevent, which have been described as ‘inadequate’ and ‘an exercise in box-ticking’<sup>1577</sup> by its attendees. Consequently, the National Union of Teachers passed a motion in March 2016 calling for Prevent to be reviewed,<sup>1578</sup> with the General Secretary stating “[e]vidence shows that grooming by extremist groups happens mainly on social media sites, not on school premises”.<sup>1579</sup> Such cases clearly highlight that, in order to apply the Prevent and Channel programmes effectively and appropriately, there needs to be in-depth training for public sector representatives, as well as an avoidance of targeting a particular group or community of people. Furthermore, a near exclusive focus on Muslim communities does not cover the backgrounds some ISIL and al-Qaeda recruits have. For example, Samantha/Sherafiyah Lewthwaite, the ‘White Widow’, was the wife of 7/7 terrorist Germaine Lindsay, and has been alleged to have been recruiting

---

<sup>1576</sup> Dodd, V. (The Guardian, 22 September 2015) *School questioned Muslim pupil about Isis after discussion on eco-activism* <<https://www.theguardian.com/education/2015/sep/22/school-questioned-muslim-pupil-about-isis-after-discussion-on-eco-activism>> accessed November 2016.

<sup>1577</sup> Jeory, T. & Cockburn, H. (The Independent, 23 July 2016) *More than 500,000 public sector workers put through Prevent counter-terror training in bid to spot extremism*, <http://www.independent.co.uk/news/uk/crime/extremism-prevent-counter-terror-training-public-sector-workers-bid-to-spot-a7152466.html>> accessed November 2016.

<sup>1578</sup> National Union of Teachers; they voted in favour of Motion 23. The General Secretary, Christine Blower, stated that: “*The NUT supports the call from the Independent Reviewer of Terrorism Legislation, David Anderson QC, and many others, for a review of Prevent. Evidence shows that grooming by extremist groups happens mainly on social media sites, not on school premises.*” National Union of Teachers *Prevent Strategy* (28 March 2016) <<https://www.teachers.org.uk/news-events/conference-2016/prevent-strategy>> accessed November 2016 <<https://www.teachers.org.uk/news-events/conference-2016/prevent-strategy>> accessed November 2016.

<sup>1579</sup> *ibid.*

women for al-Shabaab in Somalia<sup>1580</sup> and later women for ISIL in Syria,<sup>1581</sup> had a father who served in the British Army<sup>1582</sup> and did not convert to Islam until the age of 17, after her parents had separated.<sup>1583</sup> Moreover, Jack Letts, from Oxford, who went to Syria in 2014, was from a white, middle class background before leaving the UK to allegedly join ISIL,<sup>1584</sup> and his parents are currently standing trial for financing terrorism after sending him nearly £2,000 after he left for Syria.<sup>1585</sup> Grace 'Khadijah' Dare, originally from a Christian background, also converted to Islam and fled to Syria, eventually using her son in an ISIL propaganda video.<sup>1586</sup> Finally, Sally Jones aka

---

<sup>1580</sup> Pflanz, M. (The Telegraph, 8 July 2012) *Samantha Lewthwaite 'recruiting all-women terror squads'* <<http://www.telegraph.co.uk/news/worldnews/africaandindianocean/somalia/9384893/Samantha-Lewthwaite-recruiting-all-women-terror-squads.html>> accessed November 2016.

<sup>1581</sup> Akinyemi, A. (International Business Times, 28 September 2014) *White Widow Samantha Lewthwaite 'Training Isis Suicide Bombers in Syria'* <<http://www.ibtimes.co.uk/white-widow-samantha-lewthwaite-training-isis-suicide-bombers-syria-1467558>> accessed November 2016.

<sup>1582</sup> Hough, A. (The Telegraph, 29 February 2012) *Samantha Lewthwaite: 7/7 bomber widow previously a 'Home Counties' girl* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9112824/Samantha-Lewthwaite-77-bomber-widow-previously-a-Home-Counties-girl.html>> accessed November 2016; Williams, Z. (The Guardian, 27 June 2014) *The radicalisation of Samantha Lewthwaite, the Aylesbury schoolgirl who became the 'white widow'* <<https://www.theguardian.com/uk-news/2014/jun/27/what-radicalised-samantha-lewthwaite-77-london-bombings>> accessed November 2016.

<sup>1583</sup> Brown, D. (The Times, 29 February 2012) *'I just wanted to marry a Muslim and settle down'* <<http://www.thetimes.co.uk/tto/news/uk/crime/article3335196.ece>> accessed November 2016.

<sup>1584</sup> His father is a distinguished botanist and academic; Whitehead, T. (The Telegraph, 25 January 2016) *Parents of 'Jihadi Jack' speak of two years of hell and daily worry that he could die* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12120165/Parents-of-Jihadi-Jack-speak-of-two-years-of-hell-and-daily-worry-that-he-could-die.html>> accessed November 2016.

<sup>1585</sup> Boyle, D. (The Telegraph, 9 June 2016) *Parents of 'Jihadi Jack' Letts who was 'first white Briton to join Isis' remanded in custody after denying sending him money for terrorism* <<http://www.telegraph.co.uk/news/2016/06/09/parents-of-jihadi-jack-letts-who-was-first-white-briton-to-join/>> accessed November 2016; Their trial date is set for January 2017. They are alleged to have sent Mr Letts sums of money in 2014, amounting to £1,723; BBC News (17 November 2016) *'Jihadi Jack' parents to stand trial on suspicion of funding terrorism* <<http://www.bbc.co.uk/news/uk-england-oxfordshire-38015900>> accessed November 2016.

<sup>1586</sup> The boy, Isa Dare, was identified by his grandfather; Raynor, G. (The Telegraph, 4 January 2016) *'Jihadi Junior' confirmed to be Isa Dare, son of female British fanatic with links to Lee Rigby killers* <<http://www.telegraph.co.uk/news/worldnews/islamic-state/12080134/Jihadi-Junior-son-of-female-British-fanatic-with-links-to-Lee-Rigby-killers.html>>; Boulton D. (The Independent, 4 January 2016) *Child in Isis video is 'son of female British fanatic' with links to Lee Rigby killers* <<http://www.independent.co.uk/news/uk/home-news/isa-dare-isis-video-grace-khadija-dare-lee-rigby-a6796376.html>> accessed November 2016.

“Mrs Terror”, an infamous ISIL recruiter, propagandist and UN-designated individual,<sup>1587</sup> who made a series of credible social media threats to British cities during the summer of 2016,<sup>1588</sup> left the UK for Syria in 2013 with her son after striking up an online relationship with Junaid Hussein.<sup>1589</sup> All of these cases highlight that extremists and terrorists can come from different backgrounds, with recruiters from IS and al-Qaeda being experts in exploiting weaknesses and vulnerability, therefore UK authorities and practical programmes such as Prevent and Channel should be focusing on vulnerability to extremist or terrorist groups, for families and communities of all races and religions, rather than just one.

#### 5.4. Cybercrime

As with the US, cybercrime is a growing part of criminal activity in the UK and significantly, of crime with suspected links to terrorist finances. For example, in 2015, it was estimated that £398.2 million was lost to card not present fraud,<sup>1590</sup> a rise of 20% from 2014.<sup>1591</sup> Out of this, trends suggest that there has been a substantial rise

---

<sup>1587</sup> UN Security Council *Consolidated United Nations Security Council Sanctions List*, 62; her reference number is QDi.360, updated November 2016 <<https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>> accessed November 2016; she is also No. 179 on the Home Office *Consolidated List of Targets* <<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>> accessed November 2016; she is 453 on the US's Specially Designated Nationals List as well; US Department of The Treasury *Specially Designated Nationals List* (Office of Foreign Assets Control) <<https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>> accessed November 2016.

<sup>1588</sup> Sims, A. (The Independent, 25 May 2016) *Sally Jones: Isis recruiter 'issues series of terror threats against UK cities' over Twitter* <<http://www.independent.co.uk/news/world/middle-east/sally-jones-isis-recruiter-issues-series-of-terror-threats-to-uk-cities-over-twitter-a7049066.html>> accessed November 2016.

<sup>1589</sup> Shute J. (The Telegraph, 9 January 2016) *How Isil are preying on female converts in Britain to make them into jihadi brides* <<http://www.telegraph.co.uk/news/worldnews/islamic-state/12089882/How-Isil-are-preying-on-female-converts-in-Britain-to-make-them-into-jihadi-brides.html>> accessed November 2016; Khadija Dare, whose son was used as an executioner in an IS video, is also cited as another person who was enticed online.

<sup>1590</sup> Financial Fraud Action UK *Fraud: The Facts 2016* <<https://www.financialfraudaction.org.uk/fraudfacts16/>> accessed November 2016.

<sup>1591</sup> *ibid.*

in fraud against online retailers who are based abroad, of 27% since 2014, to £103million.<sup>1592</sup> Moreover, the use of identity theft in card fraud has risen in the UK in 2015 by 28%, totalling £38.2 million.<sup>1593</sup> Thus, it is clear that the rising use of the Internet to commit financial fraud, which could end up financing terrorist acts, must be addressed. The UK is again similar to the US, using various tactics available to law enforcement authorities, such as confiscation of assets and ‘Know Your Customer’ rules for financial institutions.

#### **5.4.1. Cyberlaundering**

Like the US, the UK uses traditional anti-money laundering techniques in order to trace terrorist financing through cybercrime, a difficulty because anti-money laundering laws *work back* from the crime, whereas the aim of anti-terrorism law is to *prevent* the act from happening.<sup>1594</sup> Primarily, the UK uses the Proceeds of Crime Act 2002 in order to address the issue of cyberlaundering, with s. 327 overall stating that it is an offence if a person conceals, disguises, converts or transfers criminal property,<sup>1595</sup> s. 328 creating an offence for facilitating the acquisition or use of criminal property<sup>1596</sup> and it is an offence under s. 329 to acquire, use or have possession of criminal property.<sup>1597</sup> Furthermore, these are supported by the Money Laundering Regulations, which apply the Third EU Money Laundering Directive, including having ‘Customer Due Diligence’ measures for financial institutions,<sup>1598</sup> and record-keeping.<sup>1599</sup> There

---

<sup>1592</sup> *ibid.*

<sup>1593</sup> *ibid.*

<sup>1594</sup> Gouvin, E.J., *Bringing out the big guns: The USA PATRIOT Act, Money Laundering and the war on Terrorism* (2003) 55 *Baylor Law Review* 956, 973.

<sup>1595</sup> Proceeds of Crime Act 2002 c.29, s. 327(1)(a)-(d).

<sup>1596</sup> Proceeds of Crime Act 2002 c.29, s. 328(1).

<sup>1597</sup> Proceeds of Crime Act 2002 c.29, s. 329(1)(a)-(c).

<sup>1598</sup> Money Laundering Regulations 2007 SI 2007/2157, s. 7.

<sup>1599</sup> Money Laundering Regulations 2007 SI 2007/2157, s. 19.



have been a number of successes under the Money Laundering Regulations, through the Joint Money Laundering Intelligence Taskforce, established in 2015,<sup>1600</sup> which between 2015 and April 2016 had arrested 21 individuals suspected of money laundering, instigated 544 bank-led investigations into customers suspected of money laundering, identified 1999 suspicious accounts, as well as closing 336 bank accounts and confiscation of £583,000 of suspected criminal finances.<sup>1601</sup> Furthermore, the Financial Conduct Authority (FCA) has levied significant fines against financial institutions with weak anti-money laundering provisions, ranging from £525,000<sup>1602</sup> to £8.75m.<sup>1603</sup> Additionally, in 2015, the FCA fined Barclays Bank plc £72m for failing to minimise the risk of financial crime in a £1.88billion transaction, because they had

---

<sup>1600</sup> Under the Crime and Courts Act 2013 c.22, the National Crime Agency was established and the Joint Money Laundering Intelligence Taskforce was launched as a one year pilot, providing assistance to banks and police <<http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit>> accessed November 2016.

<sup>1601</sup> *ibid.*

<sup>1602</sup> Guaranty Trust Bank (UK) Ltd was fined £525,000 in 2013 for failing to apply anti-money laundering controls to high risk customers between 2008 and 2010. The FCA found that they had failed to assess or document “*potential money-laundering risks posed by higher risk customers; Screen prospective customers against sanction lists or databases of PEPs [Politically Exposed Persons]... Review the activity of higher risk customers’ accounts and check that the information they held on these customers was up to date.*”; Financial Conduct Authority *FCA fines Guaranty Trust Bank (UK) Ltd £525,000 for failures in its anti-money laundering controls* (9 August 2013) <<https://www.fca.org.uk/news/press-releases/fca-fines-guaranty-trust-bank-uk-ltd-%C2%A3525000-failures-its-anti-money-laundering>> accessed November 2016.

<sup>1603</sup> Coutts & Co. Bank, a private owned by the Royal Bank of Scotland and with customers such as the Queen, was fined £8.75m (a 30% discount from the original £12.5m fine for settling early) for serious failures to implement anti-money laundering provisions, with deficiencies in nearly three quarters of high risk customer files; Financial Services Authority (the predecessor to the Financial Conduct Authority) *Final Notice Coutts and Company* (Reference Number 122287) (23 March 2012) <<https://www.fca.org.uk>> accessed November 2016; The FSA carried out checks on 103 customer files and identified deficiencies in 73 of those files (71%); Financial Conduct Authority (July 2013) *Anti-money laundering annual report 2012/13* <<https://www.fca.org.uk/publication/corporate/anti-money-laundering-report.pdf>> accessed November 2016; BBC News (26 March 2012) *Coutts fined for failings in money laundering controls* <<http://www.bbc.co.uk/news/business-17512140>> accessed November 2016; Treanor, J. (The Guardian, 26 March 2012) *Queen's banker fined for poor money laundering checks* <<https://www.theguardian.com/business/2012/mar/26/coutts-fined-money-laundering-checks>> accessed November 2016; Goodman, M. (The Telegraph, 29 March 2012) *Coutts agrees to settle FSA fine for reduced fee* <<http://www.telegraph.co.uk/finance/personalfinance/expand-money/9173401/Coutts-agrees-to-settle-FSA-fine-for-reduced-fee.html>> accessed November 2016.

not asked for specific information from the clients to comply with financial crime requirements for the transaction.<sup>1604</sup> Consequently, it is clear that there has been a focus on penalising financial institutions for failing to comply with the standards set out in the AML/CTF legislation.

However, as mentioned in chapter four, various means of avoiding these measures have been highlighted in *R v Tsouli, Mughal and Al-Daour*,<sup>1605</sup> in which the defendants used online casinos and stolen credit cards to launder money and eventually finance terrorism. Without physical face-to-face identification, it is relatively easy for cybercriminals to open an online account, which is vastly different to the difficulty for law enforcement to trace it back to them.<sup>1606</sup> Consequently, the European Union has now introduced the Fourth Money Laundering Directive,<sup>1607</sup> effective from 26 June 2015,<sup>1608</sup> which is aimed at ‘toughening up’ the anti-money laundering regime

---

<sup>1604</sup> Financial Conduct Authority *FCA fines Barclays £72 million for poor handling of financial crime risks* (26 November 2015) <<https://www.fca.org.uk/news/press-releases/fca-fines-barclays-%C2%A372-million-poor-handling-financial-crime-risks>> accessed November 2016.

<sup>1605</sup> *R v Tsouli, Mughal and Al-Daour* [2007] EWCA Crim 3300; Younis Tsouli (“irhaby007”), Waseem Mughal and Tariq Al-Daour raised £1.8million to finance a large number of websites and chat rooms which incited acts of terrorism; *Attorney General's References (Nos.85, 86 & 87 of 2007)*, Re 2007 WL 4368169, [5]; Jacobson, M. *Terrorist Financing and the Internet* (2010) *Studies in Conflict & Terrorism*, 33:4, 353-363, 355.

<sup>1606</sup> Hunt, J. *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them* (2011) 20(2) *Information & Communications Technology Law* 133, 136.

<sup>1607</sup> Directive 2015/849/EU (20 May 2015) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (‘Fourth Money Laundering Directive’).

<sup>1608</sup> Member States have until 26 June 2017 to transpose the new requirements into law – the UK Government has sent this out to consultation and is in the process of transposing the new Regulations; HM Treasury *Transposition of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016.

across Europe<sup>1609</sup> and recognises the anonymity that online transactions pose.<sup>1610</sup> For instance, the Directive now suggests a centralised bank and payment account register to increase access to information by Financial Intelligence Units,<sup>1611</sup> a requirement for a central register of all beneficial ownership, potentially providing up to date information on businesses<sup>1612</sup> as well as a strict prohibition of anonymous bank accounts and passbooks.<sup>1613</sup> There is also a review of customer due diligence, taking away the automatic right of simplified due diligence for certain customers, for example, financial institutions or a company on the regulated market,<sup>1614</sup> capturing banks which have been under suspicion, such as Al Rahji Bank, in connection with HSBC. The Directive also focuses on information-sharing and easier access to information by Financial Intelligence Units (FIUs), such as the National Crime Agency, through ensuring that information held by the Member State can be accessed in a ‘*timely manner*’,<sup>1615</sup> and that information would be exchanged between FIUs throughout the Union.<sup>1616</sup> Furthermore, the Directive places restrictions on the gambling industry as a whole, not

---

<sup>1609</sup> European Parliament *Parliament toughens up anti-money laundering rules* (European Parliament, 11 March 2014) <<http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38110/html/Parliament-toughens-up-anti-money-laundering-rules>> accessed November 2016; European Commission *Anti-Money Laundering: Stronger rules to respond to new threats* (Europa.eu, 5 February 2013) <[http://europa.eu/rapid/press-release\\_IP-13-87\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-13-87_en.htm?locale=en)> accessed November 2016.

<sup>1610</sup> Directive 2015/849/EU (20 May 2015) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (‘Fourth Money Laundering Directive’).

<sup>1611</sup> Directive 2015/849/EU, para. 57.

<sup>1612</sup> *ibid* Article 30(1) and (3).

<sup>1613</sup> *ibid* Article 10(1).

<sup>1614</sup> *ibid* Article 15(2), which states: “*Before applying simplified customer due diligence measures, obliged entities shall ascertain that the business relationship or the transaction presents a lower degree of risk*”.

<sup>1615</sup> *ibid* Article 32(4) and (2).

<sup>1616</sup> *ibid* Articles 51 (exchange of information through the Commission), Article 52 (Member States to ensure co-operation to the fullest extent) and Article 53 (exchange of information on request).

just casinos, taking into account the problems that *Tsouli* highlighted, including enhanced customer due diligence measures for transactions higher than €2,000, including collections of winnings or a stake.<sup>1617</sup> Finally, and most importantly, the reach of the Directive will now potentially extend to virtual currencies,<sup>1618</sup> widening the scope for its application to digital currencies such as Bitcoin.<sup>1619</sup> Such a move would open up Virtual Currency Exchange Platforms to not only apply AML and CTF measures, but also have mandatory registration or licensing requirements,<sup>1620</sup> closing further loopholes for terrorist financiers to channel their money. These strides have been significant, potentially enabling Financial Intelligence Units from across Europe to access and decipher information which inevitably passes through several countries. Although the UK is yet to implement the Directive through secondary legislation,<sup>1621</sup> this

---

<sup>1617</sup> *ibid* para. 21.

<sup>1618</sup> *ibid* Article 3(3). The European Banking Authority has accepted the European Commission's proposals to include virtual currencies under the scope of the Fourth Directive, and has published an opinion for amendments to be made to the Directive to include virtual currency platforms by the EU Parliament, the EU Commission and EU Council; *Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)* (11 August 2016) <<https://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-commission-s-proposal-to-bring-virtual-currency-entities-in-the-scope-of-the-anti-money-laundering-directive>> accessed November 2016.

NB. The European Commission already states that virtual currencies fall within the scope of the AML Directive; European Commission *Questions and Answers: Money Laundering Directive Factsheet* (Europa.eu, 5 July 2016) <[http://europa.eu/rapid/press-release MEMO-16-2381\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm)> accessed November 2016.

<sup>1619</sup> Chapter four, 4.3.1.

<sup>1620</sup> *ibid* *Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*, 2, para. 6.

<sup>1621</sup> NB. The Criminal Finance Bill 2016-17 is going through Parliament, which should address some of the Fourth Anti-Money Laundering Directive's measures. This is set to be a powerful tool in the fight against money laundering; UK Parliament Criminal Finances Bill 2016-17 <<http://services.parliament.uk/bills/2016-17/criminalfinances.html>> accessed November 2016. The issue of Brexit may also come into play, yet the UK has previously gold-plated AML Directives and, in 2016, agreed on the issue of a central register for beneficial owners; Department for Business, Innovation and Skills, *Enhancing Transparency of Beneficial Ownership Information* (March 2016) <<https://www.gov.uk/.../uploads/.../bis-16-161-beneficial-ownership-transparency.pdf>> accessed November 2016; furthermore, there has been discussion of a Fifth Anti-Money Laundering Directive; European Commission *Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering* (Europa.eu, 5 July 2016) <[http://europa.eu/rapid/press-release IP-16-2380\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2380_en.htm)> accessed November 2016.

is an area which may allow more effective investigation of money laundering and terrorist financing through the Internet.

Yet, despite its potential effectiveness, the application of the Directive will potentially cost businesses in the UK £26m a year to apply.<sup>1622</sup> This financial burden is potentially offset by both the amount of businesses affected by Anti-Money Laundering provisions, 150,000 or 3%,<sup>1623</sup> and the amount of finances generated by UK organised crime, estimated by the Home Office to be £13billion in 2011-12<sup>1624</sup> and by the EU to be €25billion.<sup>1625</sup> Furthermore, the amount of money laundered in the UK, again estimated by the Home Office to be £10.5billion,<sup>1626</sup> although this excludes 85% of fraud and other non-organised crime.<sup>1627</sup> However, as also noted before, the fines levied against financial institutions can be substantial for non-compliance with AML and CTF requirements.<sup>1628</sup> Both the cost of AML and CTF procedures as well as the fines incurred by financial institutions means that banks have become more risk-averse to some customer accounts, potentially limiting the appropriateness of their measures to counteract money laundering and terrorist financing. This is compounded by the fact that, under the Third Money Laundering Directive, reporting requirements come into action when the financial institution knows or ‘suspects’ money laundering or

---

<sup>1622</sup> Home Office *Impact Assessment of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016.

<sup>1623</sup> *ibid* 6, para. 25.

<sup>1624</sup> *ibid* 3, para. 3; Mills, H. Skodbo, S. and Blyth, P., (Home Office) *Understanding organised crime: estimating the scale and the social and economic costs* (7 October 2013) <<https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs>> accessed November 2016.

<sup>1625</sup> Project ECOLEF *The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy* (February 2013), 39 <[http://www2.econ.uu.nl/users/unger/ecolef\\_files/Final%20ECOLEF%20report%20\(digital%20version\).pdf](http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf)> accessed June 2018.

<sup>1626</sup> *ibid* *Understanding organised crime: estimating the scale and the social and economic costs*.

<sup>1627</sup> *ibid*.

<sup>1628</sup> FCA’s £72m fine of Barclays Bank plc, Financial Conduct Authority *FCA fines Barclays £72 million for poor handling of financial crime risks* (26 November 2015) <<https://www.fca.org.uk/news/press-releases/fca-fines-barclays-%C2%A372-million-poor-handling-financial-crime-risks>> accessed November 2016.

terrorist financing is being committed.<sup>1629</sup> As noted under section 5.3.2. of this chapter, several Non-Governmental Organisations (NGOs) who work in high risk areas, have had their bank accounts frozen because of banks' suspicion, meaning that vital aid was not delivered to certain countries.<sup>1630</sup> Furthermore, the Financial Ombudsman Service deals with, on average, 20-30 complaints a week about the closure of personal accounts due to AML risk procedures by financial institutions,<sup>1631</sup> mainly because the banks had not communicated reasons for the closures with them.<sup>1632</sup> The over-zealous nature of financial institutions in offsetting their risk may become more prevalent when AML/CTF is extended under the Fourth Directive.<sup>1633</sup> It is therefore important to ensure that, while banks and financial institutions, as well as money services businesses and gambling institutions have a framework to apply anti-money laundering measures, they have a sufficient balance to ensure their suspicions do not penalise legitimate customers.

#### **5.4.2. Online Fraud**

As noted before, the prevalence of online fraud is still increasing and is set to increase further with growing dependence of customers on Internet transactions and online

---

<sup>1629</sup> Directive 2005/60/EC (26 October 2005) on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing ("Third Money Laundering Directive"), Article 22(1).

<sup>1630</sup> E.g. Ummah Welfare Trust was told by HSBC that their account was to be closed and another NGO had to forego £2million in donations because their bank had blocked their funds; Overseas Development Institute *UK humanitarian aid in the age of counterterrorism: perceptions and reality* (March 2015) <<https://www.odi.org/publications/9301-counter-terrorism-legislation-law-uk-muslim-ngos-charities-commission-humanitarian>> accessed November 2016.

<sup>1631</sup> Artington, D., Dove, N., Howell, J. & Levi, M. *Drivers & Impacts of Derisking A study of representative views and data in the UK* (John Howell & Co. Ltd. for the Financial Conduct Authority, February 2016) <<https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking>> accessed November 2016.

<sup>1632</sup> *ibid.*

<sup>1633</sup> NB. The UK Government is still consulting on the Fourth Money Laundering Directive, which includes the Customer Due Diligence for e-money; HM Treasury *Transposition of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016.

banking. For example, in March 2016, Financial Fraud Action UK found that overall fraud had increased by 26% in 2015, with fraudsters stealing a total of £755million in the UK.<sup>1634</sup> Additionally, Internet banking fraud had increased by 64%, with £133million being stolen from customers in 2015 alone, nearly triple the amount taken in 2011.<sup>1635</sup> The UK's Fraud Act 2006 provides some action against online fraud, with s. 2 on fraud by false representation including representation "*submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)*",<sup>1636</sup> capturing such actions as 'phishing', or masquerading as an official organisation to gain personal information,<sup>1637</sup> as well as entering a number into a 'Chip and PIN' machine.<sup>1638</sup> However, the Fraud Act's provisions are limited by territorial provision,<sup>1639</sup> reducing the effectiveness this will have in capturing those fraudulent acts across international borders, and their subsequent use in terrorist activities.

International co-operation on these matters is therefore key to ensuring that fraud relating to terrorist financing is found. The European Convention on Cybercrime<sup>1640</sup> has partly addressed this issue,<sup>1641</sup> although the UK only ratified its terms in 2011, more than 11 years after it was introduced.<sup>1642</sup> Indeed, ratifying the European

---

<sup>1634</sup> Financial Fraud Action UK *Year-end 2015 fraud update: Payment cards, remote banking and cheque* (17 March 2016) <<https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/downloads-7-3085-2015-year-end-fraud-update-report.pdf>> accessed November 2016.

<sup>1635</sup> *ibid.* In 2011, £51.2m was taken from online bank accounts.

<sup>1636</sup> Fraud Act 2006 c. 35, s. 2(5).

<sup>1637</sup> Fraud Act 2006 c.35, Explanatory Notes, para. 16.

<sup>1638</sup> *ibid.* para. 17.

<sup>1639</sup> *ibid.* – this only applies to England, Wales and Northern Ireland. There are no extra-territorial provisions to the Act.

<sup>1640</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001) <<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>> accessed November 2016.

<sup>1641</sup> *ibid.* E.g. International Co-operation under Title III, Article 23.

<sup>1642</sup> *ibid.* European Treaty Series No. 185 Convention on Cybercrime (23 November 2001).

Convention on Cybercrime is a useful tool in policing the Internet<sup>1643</sup> and combating cross-border issues,<sup>1644</sup> along with placing a stronger duty upon ISPs to monitor communications.<sup>1645</sup> Yet, it is limited to those countries which have ratified its aims, and many other European Union Member States have delayed further the ratification of the Convention than the UK, including Austria in 2012,<sup>1646</sup> Belgium in 2012,<sup>1647</sup> Luxembourg in 2014<sup>1648</sup> and Poland in 2015,<sup>1649</sup> meaning that its provisions will have been applied in a patchy manner at a regional level. As outlined previously, the use of the Internet provides the cybercriminal with distinct advantages, such as spreading their crimes over multiple jurisdictions.<sup>1650</sup> As the House of Lords Science and Technology Committee commented as far back as 2007, “*no law enforcement agency can combat e-crime effectively in isolation, but the mechanisms for international co-operation are inefficient and slow moving...*”.<sup>1651</sup> Consequently, without international authority, the effectiveness of law enforcement is limited. As the Committee subsequently recommended, many of these problems could be counteracted by setting up an online reporting system which could collect data and provide reports regarding cybercrime.<sup>1652</sup> Therefore, the use of such recommendations could also identify the extent to which terrorists fund their activities through cybercrime, which would enhance

---

<sup>1643</sup> Jarvie, N. *Control of Cybercrime – is an end to our privacy on the Internet a price worth paying?* Part 2 (2003) 9(2) Computer and Telecommunications Law Review 110, 110.

<sup>1644</sup> *ibid*; House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007), 64 <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016.

<sup>1645</sup> Jarvie, N. *Control of Cybercrime – is an end to our privacy on the Internet a price worth paying?* Part 2 (2003) 9(2) Computer and Telecommunications Law Review 110, 114; Cybercrime Convention 2001 Article 16(2).

<sup>1646</sup> *ibid*.

<sup>1647</sup> *ibid*.

<sup>1648</sup> *ibid*.

<sup>1649</sup> *ibid*.

<sup>1650</sup> *ibid* Jarvie, N., 112.

<sup>1651</sup> House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007), 64 <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016.

<sup>1652</sup> *ibid* 78, paras. 7.75-7.76.



effectiveness.<sup>1653</sup>

Since then, the Government has attempted to increase the success of the AML and CTF scheme, with a complete review of powers, including the effectiveness of Suspicious Activity Reports and international co-operation. As part of the *Action Plan for anti-money laundering and counter-terrorist finance*,<sup>1654</sup> not only is there a schedule for legislation to provide a framework for information-sharing between public and private entities for 2017.<sup>1655</sup> Furthermore, the Anti-Corruption Summit in 2016 has attempted to increase the use of information-sharing, with the European Commission outlining its support under the Fourth Money Laundering Directive.<sup>1656</sup> However, the United Nations and World Bank fell silent on this matter, instead concentrating on “building accountable and transparent criminal justice systems”<sup>1657</sup> and “support for the implementation of international accounting and auditing standards, encouraging the adoption of better fiscal transparency practices through active participation in international forums”.<sup>1658</sup> While these are notable and powerful aims, without the ability of Financial Intelligence Units and financial institutions to share their knowledge with ease, the loopholes of online fraud will continue to be exploited.

Finally, in order to counteract the problem of using traditional techniques for hi-tech crimes, data retention is a valuable tool for law enforcement agencies when

---

<sup>1653</sup> NB. The UK Government at the time did not accept these recommendations; House of Lords Science and Technology Committee, *Personal Internet Security: A Follow Up*, 4<sup>th</sup> Report of Session 2007-8 (8 July 2008), 5.

<sup>1654</sup> Home Office *Action Plan for anti-money laundering and counter-terrorist finance* (April 2016) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/517992/6-2118-Action\\_Plan\\_for\\_Anti-Money\\_Laundering\\_web\\_.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering_web_.pdf)> accessed November 2016.

<sup>1655</sup> *ibid* 5.

<sup>1656</sup> Cabinet Office *Anti-Corruption Summit: regional and international organisation statements* (12 May 2016) <<https://www.gov.uk/government/publications/anti-corruption-summit-regional-and-international-organisation-statements>> accessed November 2016.

<sup>1657</sup> *ibid* United Nations Statement, para. 9.

<sup>1658</sup> *ibid* World Bank Statement, at point 1.

detecting terrorist financing over the Internet.<sup>1659</sup> Following 9/11, the introduction of ATCSA allowed the UK to impose a legislative framework on data retention for the first time. Under Part 11 of ATCSA, the Secretary of State is authorised to issue a code of practice, allowing the retention of personal communications data for purposes of national security or the prevention or detection of crime, or the prosecution of offenders.<sup>1660</sup> The introduction of such measures seems to be in line with the law enforcement agency argument that “...*the availability of such data is often crucial to the successful investigation of crimes committed by means of telecommunications networks...*”.<sup>1661</sup> However, the retention of data by Internet Service Providers is *voluntary*, not obligatory<sup>1662</sup> and is only conducted on a temporary basis,<sup>1663</sup> counteracting the effectiveness of such a provision. Consequently, law enforcement agencies have been limited in their effectiveness through these measures in tracking personal communications data.

Yet, as noted before, the use of data retention and surveillance has been before the CJEU,<sup>1664</sup> as well as before the ECtHR.<sup>1665</sup> As the UK is set to go further with its

---

<sup>1659</sup> Vilasau, M. *Traffic Data Retention v Data Protection: the new European Framework* (2007) Computer Technology Law Review 13(2) 52, 52; Data Protection Act 1998 c.29, Data Protection Principles, Principle 5.

<sup>1660</sup> Anti-terrorism, Crime and Security Act 2001 c.24, s. 102(5) (a) and (b).

<sup>1661</sup> Breyer, P. *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR* (2005) 11 European Law Journal 3, 365.

<sup>1662</sup> Nettleton, E. & Watts, M. *Legal update: The Data Retention Directive* (2006) 14 Database Marketing and Consumer Strategy Management 74, 75; Donohue, L. K. *Anglo-American Privacy and Surveillance* (2005-6) 96 Journal of Criminal Law and Criminology 1059, 1182.

<sup>1663</sup> *ibid* Donohue, L. K., 1181.

<sup>1664</sup> Case C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and others. *Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221; Case C-698/15 *Home Secretary v Tom Watson, Peter Brice, Geoffrey Lewis – Intervening Parties: Open Rights Group, Privacy International, The Law Society of England and Wales.*

<sup>1665</sup> *Roman Zakharov v Russia* (Application no. 47143/06) (Court (Grand Chamber)), [2015] ECHR 1065; *Szabó and Vissy v Hungary* (Application no. 37138/14) (Court (Fourth Section)), [2016] ECHR 579.

data retention scheme than both EU members and other members of the ‘Five Eyes’ surveillance system,<sup>1666</sup> including the US through the Investigatory Powers Act, it remains to be seen that, while it is likely to be an effective tool, it is unlikely to be an appropriate one, given that both the CJEU and the ECtHR have placed significant barriers in its way.

### **5.5. Conclusion:**

The UK reacted in much the same way as the US after 9/11, broadening its anti-financial crime powers and using surveillance measures on Internet communications. Yet, it had one distinct advantage. Its history of terrorism and CTF had broadly paved the way for finding ways in which terrorists can channel and raise finances, which can ostensibly be used for Internet transactions, and making it more effective. Through understanding that terrorist financing is a separate offence to money laundering, law enforcement has taken a more preventative approach towards terrorist financing, rather than working back from the crime; an inherent disadvantage of using AML for CTF offences. Moreover, the UK went further than the US after the 7/7 bombings, attempting to address the problems inherent with ‘cheap terrorism’ and looking towards a preventative strategy, to stop people from becoming radicalised and therefore attempting to stem the tide of financing and support for terrorist organisations. However, its application has been severely criticised on the basis that it has focused too much on one section of society, Muslim communities, that it should refocus its aims to prevent radicalisation and extremism to all those who are most vulnerable and susceptible to such propaganda. Additionally, a more intensive training programme for

---

<sup>1666</sup> ibid Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), 265, 14.30 <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018 - “such obligations were not considered politically conceivable by [his] interlocutors in Germany, Canada or the US”.

teachers and other public sector workers dealing with vulnerable people, would go some way to satisfying concerns about the appropriateness of the Prevent Strategy.

The UK also falls into the same trap as the US when finding terrorist financing. By relying on the SARs system too much, there is a danger that vital information may be missed under the sheer weight of reporting, not helped by a weak Government response when banks such as HSBC knowingly collude in failing to report suspicious transactions with sanctioned states. This problem multiplies substantially if one takes into account Internet transactions, due to the millions of transactions made daily. It is an impossible task for both financial institutions and law enforcement authorities to sift through the information available. Furthermore, the UK legislative framework suffers from weaknesses not found in the US. For instance, it still does not use intercept evidence in courts. This is an effective way of ensuring that convictions are sound and provides an appropriate level of supervision by the justice system as to whether surveillance is defensible. Through introducing intercept evidence, compatible with Article 6 ECHR, the UK could substantially increase the effectiveness of its conviction rate when dealing with terrorist communications.

Most importantly, the UK has also stepped far beyond the US and its obligations under the European Convention on Cybercrime in its surveillance measures. Instead of rolling back intrusive surveillance powers over Internet communications after the Snowden revelations, as happened with the US and the EU, the UK introduced the Investigatory Powers Act, squarely aimed at keeping data retention and mass surveillance powers, as well as extending these powers further. The UK has also introduced website filtration without a supporting legal framework or judicial oversight, through ISPs operating in the UK adopting an 'opt in' system for new broadband customers.

Again, this contradicts the more protective nature the US and the EU have taken towards freedom of speech and expression and takes the UK on a collision course with both the CJEU and the ECtHR, as well as taking away the balance with human rights obligations outlined by the European Convention on Cybercrime. Indeed, it seems that the UK is now heading towards more control of Internet communications, as routinely happens in Saudi Arabia. While the UK does not have anywhere near the level of control available to the Saudi Government and law enforcement authorities, given that its telecommunications network is privately owned, it is concerning that it is heading down the road of filtration as a means of preventing radicalisation.

## **Chapter Six: Saudi Arabia**

*“Whether it is non-state actors like Al-Qa’ida, the terror-state “Daesh”/ISIL, or state-sponsored terror from Iran and its proxies, Saudi Arabia has as much as any other country a national security incentive to stop the men, the money, and the mind-set that inspire and incite violent extremism.”*<sup>1667</sup>

### **6.1 Introduction**

Saudi Arabia has been paradoxical in its efforts to combat terrorist financing, as well as in its relationship with the main driver of post 9/11 CTF provisions, the United States (US), being described by the 9/11 Commission as “*a problematic ally in combating Islamic extremism*”.<sup>1668</sup> While international relations between the two countries have flourished on trade, particularly arms and security,<sup>1669</sup> Saudi Arabia has also been a country susceptible to al-Qaeda.<sup>1670</sup> There have also been some concerns from the US about Saudi’s human rights records<sup>1671</sup> and, more recently, the passing of a Bill by the US Congress, which allows families of 9/11 victims to sue Saudi authorities for their alleged part in the preparation of the attacks<sup>1672</sup> has changed the relationship further.

---

<sup>1667</sup> *The Kingdom of Saudi Arabia and Counter-terrorism 2016*, available through Saudi-U.S. Trade Group *The Kingdom of Saudi Arabia and Counter-terrorism 2016 (Comprehensive Document Outlining Saudi Arabia’s Counterterrorism Strategy, Successes Released )* (26 May 2016) <<http://sustg.com/comprehensive-document-outlining-saudi-arabias-counterterrorism-strategy-successes-released/>> accessed November 2016.

<sup>1668</sup> *9/11 Commission Report* (22 July 2004), 371 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1669</sup> Blanchard, C. RL33533 *CRS Report to Congress Saudi Arabia: Background and U.S. Relations* (20 September 2016), 1 <<https://fas.org/sgp/crs/mideast/RL33533.pdf>> accessed June 2018.

<sup>1670</sup> *ibid* *9/11 Commission Report* (22 July 2004), 371.

<sup>1671</sup> *ibid* Blanchard, C..

<sup>1672</sup> Smith, D. (The Guardian, 29 September 2016) *Congress overrides Obama’s veto of 9/11 bill letting families sue Saudi Arabia* <<https://www.theguardian.com/us-news/2016/sep/28/senate-obama-veto-september-11-bill-saudi-arabia>> accessed November 2016.

The 9/11 Commission Report also identified Saudi Arabia as a country vulnerable to channelling funds by al-Qaeda and other terrorist organisations,<sup>1673</sup> due to its complex system of banking, sparse record-keeping and charitable donations to organisations with terrorist links.<sup>1674</sup> In 2002, the Council on Foreign Relations was blunter about Saudi involvement, stating that “[f]or years, individuals and charities based in Saudi Arabia have been the most important source of funds for al-Qaeda. And for years, Saudi officials have turned a blind eye to this problem”.<sup>1675</sup> Yet, the 9/11 attacks were not the ‘watershed’ moment for the Saudi Arabian authorities to immediately tackle money laundering and terrorist financing as they had been for, particularly, the US. Instead, it was not until after the 2003 terrorist bombings in Riyadh that Saudi Arabia attempted to conform to international standards to detect and prevent terrorist financing.<sup>1676</sup> For example, Saudi Arabia signed up to the Financial Action Task Force’s (FATF) recommendations for terrorist financing, through becoming a member of the FATF in the Middle East, the Middle East North Africa Financial Action Task Force (MENAFATF)<sup>1677</sup> and entered into a number of bilateral agreements with the United States (US). Additionally, with the rise of ISIL in Syria, Saudi Arabia has been at the forefront of international efforts to combat their financing and support, including co-chairing the Counter-ISIL Finance Group with the US and Italy since

---

<sup>1673</sup> *ibid* 9/11 Commission Report (22 July 2004), 371-2 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1674</sup> *ibid* 170-171.

<sup>1675</sup> Council on Foreign Relations *Terrorist Financing* (Chairman Maurice R. Greenberg, 2002), [1] <<http://www.cfr.org/terrorist-financing/terrorist-financing/p5080>> accessed November 2016.

<sup>1676</sup> Riyadh Declaration 5-8 February 2005; Saudi Arabian Ministry of Foreign Affairs *Counter-Terrorism International Conference* (26 October 2009) <<http://www.mofa.gov.sa/sites/mofaen/Kingdom-ForeignPolicy/AntiTerrorism/Pages/AntiTerrorismConference35026.aspx>> accessed November 2016.

<sup>1677</sup> MENAFATF Members <<http://www.menafatf.org/topiclist.asp?ctype=about&id=430>> accessed November 2016.

2015.<sup>1678</sup> Therefore, the requirements which the Saudi AML/CTF Rules 2003 place on banks and financial institutions will be examined, as well as whether these are effective and preventing terrorist financing when using a virtually anonymous medium such as the Internet. Furthermore, with nearly 21 million Saudi Arabians having access to the Internet, or approximately 65% of the population,<sup>1679</sup> Saudi Arabia has a fast-growing number of Internet users and, combined with the country's wealth and the mandatory charitable tax, zakat, creates large Internet transactions annually, with e-commerce alone generating \$2billion of transactions in 2015.<sup>1680</sup> Therefore, there will be an appraisal of whether Saudi measures against charitable organisations are effective when directly solicited over the Internet, or whether there is more of a reliance on face-to-face transactions in order for CTF to work. Finally, throughout, there will be an assessment on whether Saudi Arabia has appropriately balanced its methods of tracing terrorist finances through the Internet with its own laws on privacy. Furthermore, there will be a comparison with the US and United Kingdom (UK), both of which have a higher level of privacy and freedom of expression principles, to find out whether Saudi Arabia's stance is compatible, and if it will affect mutual legal assistance and extradition as outlined under Articles 15 and 17 of the 1999 Convention for the Suppression of the Financing of Terrorism.

## **6.2. Direct solicitation of donations**

---

<sup>1678</sup> US Department of State *Fact Sheet: Taking Stock of the Counter-ISIL Finance Group's Achievements in its First Year* (12 April 2016) <<http://www.state.gov/e/eb/rls/othr/2016/255765.htm>> accessed November 2016.

<sup>1679</sup> Internet Live Stats *Saudi Arabia Internet Users* accurate figures for 2016 are 20,813,695 or 64.7% as at 1 July 2016 <<http://www.internetlivestats.com/internet-users/saudi-arabia/>> accessed November 2016.

<sup>1680</sup> Payfort *State of Payments 2016* <<http://www.payfort.com/stateofpayments2016/#trends>> accessed November 2016.



After 9/11, Saudi Arabia was alleged to have links with extremist websites hosted by US-designated terrorist organisations such as Hamas, Hezbollah and al-Qaeda.<sup>1681</sup> As Levitt outlines, in July 2002, Saudi ISPs featured an ‘Islam online’ portal, openly directing users to “*support the Palestinian struggle*”<sup>1682</sup> and “*glorified suicide attacks*”,<sup>1683</sup> while providing lists of global organisations acting as a channel for transferring terrorist finances. Furthermore, the Al-Quds Intifada Committee website, which was launched by HAMAS in the wake of the breakdown in Palestine-Israeli relations in 2000,<sup>1684</sup> maintained under the name “the Saudi Committee for Relief of the Palestinian People,” contained over 40,000 transaction records featuring the names of individuals who had received humanitarian aid and support from the Committee, and of these, families of 60 Palestinian militants who carried out attacks on military personnel and civilians between 2000 and 2002 were provided with financial support.<sup>1685</sup> Therefore, Saudi Arabia had a debatable policy towards certain websites and online communications which promoted terrorist causes and solicited donations.

### 6.2.1. Websites

---

<sup>1681</sup> Weimann, G. *www.terror.net – How Modern Terrorism Uses the Internet* (March 2004) Special Report 116 United States Institute of Peace 10, 3-4 <<https://www.usip.org/sites/default/files/sr116.pdf>> accessed November 2016; US Department of State Bureau of Counterterrorism *Foreign Terrorist Organizations* <<https://www.state.gov/j/ct/rls/other/des/123085.htm>> accessed April 2018.

NB. The United Nations does not have a list of proscribed terrorist organisations.

<sup>1682</sup> Levitt, M.A. *The Political Economy of Middle East Terrorism* (Washington Institute, December 2002) 6(4) Middle East Review of International Affairs. 56 <<http://www.washingtoninstitute.org/policy-analysis/view/the-political-economy-of-middle-east-terrorism>> accessed November 2016.

<sup>1683</sup> *ibid.*

<sup>1684</sup> Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008), 132.

<sup>1685</sup> Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues* (8 December 2004, updated 14 September 2007) 15, <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

After the Riyadh bombings, Saudi Arabia immediately toughened its stance on terrorist financing, by sharing information with US intelligence services, and setting up a US-Saudi Joint Intelligence Task Force in order to assist in tracing terrorist finances.<sup>1686</sup> Moreover, in 2003, Saudi Arabia made terrorist financing and money laundering a criminal offence under its Anti-Money Laundering Law,<sup>1687</sup> stating under Article 2(d) that the “[f]inancing of terrorism, terrorist acts and terrorist organizations [sic]”<sup>1688</sup> commits the crime of money laundering.<sup>1689</sup> Clearly, progress had been made by Saudi Arabia to legislate against the direct solicitation of donations. However, it was a further four years until Saudi Arabia ratified the 1999 UN Convention for the Suppression of the Financing of Terrorism in 2007,<sup>1690</sup> creating concerns about the international effectiveness of its legislation. As the 2007 US Congressional Research Service Report revealed, despite criminalising terrorist financing, there was disappointment about the “*lack of public prosecutions for individuals accused of financing terrorism outside of the kingdom*”.<sup>1691</sup> Additionally, the FATF and the Gulf Cooperation Council visited Saudi Arabia to assess its financial practices, finding that the Saudi legal definition of terrorist financing “*does not conform to the international standards as expressed by the [1999 Convention]*”.<sup>1692</sup> Consequently, it was difficult

---

<sup>1686</sup> *ibid* 22.

<sup>1687</sup> Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003, Articles 1 and 2.

<sup>1688</sup> *ibid* Article 2(d).

<sup>1689</sup> *ibid*.

<sup>1690</sup> United Nations Treaty Collection *International Convention for the Suppression of the Financing of Terrorism* (9 December 1999) <[https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtsg\\_no=XVIII-11&chapter=18&clang=en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtsg_no=XVIII-11&chapter=18&clang=en)> accessed November 2016.

<sup>1691</sup> Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress Saudi Arabia: Terrorist Finance Issues* (14 September 2007) 27 <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

<sup>1692</sup> *ibid* Prados A.B. & Blanchard, C.M. *CRS Report to Congress Saudi Arabia: Terrorist Financing Issues* (September 2004) 19-20; Boon K.E., Huq, A. & Lovelace D.C. *Terrorism: Commentary on Security Documents Vol 106 Terrorist Financing and Money Laundering Vol. 107* (Oxford University Press, 2010), 180.

to assess whether the Saudi authorities had the capability to capture donations solicited through websites well up to 2010.

Furthermore, the 2010 MENAFATF Mutual Evaluation Report highlighted some difficulties with the overall interpretation and application of the Anti-Money Laundering Law, with Saudi Arabia found to be ‘Non-Compliant’ or ‘Partially Compliant’ on 18 out of the 40 AML/CTF Recommendations.<sup>1693</sup> Primarily, unlike the US and the UK, Saudi Arabia uses an “all crime” approach to money laundering under Shari’ah, meaning that all activity which constitutes a crime punishable under Shari’ah or statute is an automatic predicate offence for money laundering, such as terrorist financing.<sup>1694</sup> This makes it difficult to separate out the offences individuals have been convicted for in Saudi courts as they are all classed as ‘money laundering’, therefore the effectiveness of Saudi intervention on terrorist financing is virtually unknown.<sup>1695</sup> Secondly, on foreign predicate offences, which would cover the use of the Internet by terrorist organisations outside Saudi Arabia, the Report stated that the Saudi authorities believed the jurisdiction to prosecute extended to predicate offences occurring outside its jurisdiction, as long as the asset generating offence is an offence under Saudi law, a principle covered by Shari’ah.<sup>1696</sup> However, there was no case law available, which applied this principle to offences traditionally regards as money laundering.<sup>1697</sup> Consequently, it was recommended that “[t]he Saudi authorities should be more precise in the formulation of the ML criminalisation and should strive for clear

---

<sup>1693</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010) <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016.

<sup>1694</sup> *ibid* 33.

<sup>1695</sup> *ibid* 36.

<sup>1696</sup> *ibid* 33 fn. 32 “Do not transgress limits, for Allah does not love transgressors” (Qur’an 5:87) and “Help you one another in righteousness and piety, but help you not one another in sin and rancour”. The Holy Qura’n <<https://www.alislam.org/quran/>> accessed June 2018

<sup>1697</sup> *ibid* Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010).

*provisions... The authorities are also urged to make a conceptual distinction in the AMLS between the ML and TF*”,<sup>1698</sup> showing that Saudi Arabia had clear deficiencies within its legal framework to combat terrorist financing, only being partially compliant with the FATF’s (then) Special Recommendation II.<sup>1699</sup>

However, in 2013, Saudi Arabia criminalised terrorist financing as a separate offence to money laundering under the Penal Law for Crimes of Terrorism and its Financing,<sup>1700</sup> as well as implementing executive procedures to carry out the 1999 Convention.<sup>1701</sup> These seem to have been concurrent with the rise of ISIL in Syria, as well as the consequences of Arab Spring in 2011. For example, the Law provides a more detailed definition of terrorist financing under Article 1(2), broadening out the circumstances of terrorist financing, including “*collecting, giving, receiving, allocating, transporting or transferring money or its interests, either in total or in part, to any terrorist activity*”.<sup>1702</sup> Furthermore, the law increases information-sharing provisions<sup>1703</sup> and enables the Minister of the Interior to issue warrants against those suspected of this crime.<sup>1704</sup> Together, these had been deemed by the MENFATF as being ‘largely compliant’ with international regulations,<sup>1705</sup> potentially becoming more effective in tracing finances which have been solicited through websites.

---

<sup>1698</sup> *ibid* [145], 37.

<sup>1699</sup> *ibid* 37-41.

<sup>1700</sup> MENAFATF *Mutual Evaluation Report: 4th Follow-Up Report for Saudi Arabia* (17 June 2014), 4 <[http://www.menafatf.org/sites/default/files/KSA\\_Exit\\_report\\_EN.pdf](http://www.menafatf.org/sites/default/files/KSA_Exit_report_EN.pdf)> accessed June 2018.

<sup>1701</sup> Implementation of the Convention for the Suppression of the Financing of Terrorism, Ministerial Decision No. (1697) dated 20, Rabih Al-Thani 1433 A.H. (14 March 2012) which is based on the Royal Order No. (1804) dated 7, Muharram 1433 A.H. (3 Dec. 2011).

<sup>1702</sup> Penal Law for Crimes of Terrorism and its Financing 2013 Royal Decree No. M/16 of 27 December 2013, Article 1. SAMA <<http://www.sama.gov.sa/en-US/AntiMoney/Pages/RulesandRegulations.aspx>> accessed November 2016; European-Saudi Organisation for Human Rights *Law of terrorism crimes and its financing* <[http://www.esohr.org/en/?page\\_id=788](http://www.esohr.org/en/?page_id=788)> accessed November 2016.

<sup>1703</sup> *ibid* Article 14.

<sup>1704</sup> *ibid* Article 4.

<sup>1705</sup> *ibid* MENAFATF, 4.

Saudi authorities have also been proactive in countering extremist websites. In 2007, the Assistant to the Head of the Saudi National Intelligence Agency (SNIA) estimated that there were nearly 17,000 extremist websites with an increase of 9,000 websites annually that “*move away from original Islam in order to legitimize violence*”.<sup>1706</sup> Consequently, SNIA outreach to fourteen website hosting companies have been made to reduce the activities of more than 5,400 websites which have been used by terrorist organisations.<sup>1707</sup> Additionally, for many years, through the ‘Sakinah’ Campaign, “*Ministry of Interior workers or those from the Ministry of Islamic Affairs track online discussions and surf the Internet to collect material on potential extremism*”,<sup>1708</sup> and infiltrate extremist or terrorist-affiliated websites to stop radicalisation.<sup>1709</sup> Sakinah, meaning ‘tranquility’, is officially a non-governmental organisation, which provides one-on-one chats with those seeking out radical websites, trying to diffuse potential radicalisation.<sup>1710</sup> Drawing from experienced individuals who have religious, psychological and social backgrounds,<sup>1711</sup> volunteers target social media and Internet forums to confront extremist views by using a database of theological arguments to diffuse potential radicalisation.<sup>1712</sup> This has proven to be quite successful as, although no statistics are available, some of the volunteers are former extremists

---

<sup>1706</sup> Kingdom of Saudi Arabia *The Kingdom of Saudi Arabia and Counterterrorism* (2016), 35. <<https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf>> accessed November 2016.

<sup>1707</sup> *ibid.*

<sup>1708</sup> *ibid* 36.

<sup>1709</sup> *ibid.*

<sup>1710</sup> Boucek, C. *The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia* (Combating Terrorism Center, 15 August 2008) <<https://www.ctc.usma.edu/posts/the-sakinah-campaign-and-internet-counter-radicalization-in-saudi-arabia>> accessed November 2016.

<sup>1711</sup> bin Khalid al-Saud, A. *The Tranquility Campaign: A Beacon of Light in the Dark World Wide Web*, Perspectives on Terrorism Vol. 11 No. 2 (2017), <<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/596/html>>, accessed April 2018.

<sup>1712</sup> *ibid.*

who have been turned around by the programme,<sup>1713</sup> and has reached individuals outside of Saudi Arabia through its website.<sup>1714</sup> Therefore, countries who are combatting ‘cheap terrorism’, such as the UK, may wish to consider using a version of Sakinah to reach vulnerable people via social media.

Despite these more rounded efforts to combat terrorist websites, Saudi Arabia has some of the toughest Internet censorship in the world and, as Murray outlines, “*closely controls access*”.<sup>1715</sup> As noted in chapter five,<sup>1716</sup> the UK also has a broad website filtration system which is based on users opting into certain websites which may be, for example pornographic in nature, but by contrast, Saudi Arabia’s system completely blocks any access to websites it deems unlawful or immoral. Through the 2001 Internet Rules, website filtration and content blocking are allowed, with s. 8 of the Rules prohibiting Saudi citizens from publishing or accessing sites “*which incite or promote crime*” or “*advocate violence*”.<sup>1717</sup> Furthermore, ISPs which do not block these sites are open to a fine of up to SR5million under the Telecom Act 2001.<sup>1718</sup> Therefore, Saudi Arabia has the legislative framework available to combat direct solicitations of donations by terrorist organisations via websites. Nevertheless, over 85% of the websites blocked by the Communications and Information Technology Commission (CITC) in 2014 were those with sexually explicit content.<sup>1719</sup> Additionally, while Saudi Arabia is relatively open about the techniques it uses, there is no

---

<sup>1713</sup> ibid Boucek, C.

<sup>1714</sup> Sakinah Campaign Website (English) - <<http://en.assakina.com/?cat=83>> accessed 14 April 2018.

<sup>1715</sup> Murray, A. *Information Technology Law: The Law and Society* (3rd Edn. Oxford University Press, 2016), 83.

<sup>1716</sup> Chapter 5.2.1.

<sup>1717</sup> Saudi Internet Rules 2001 Council of Ministers Resolution 12 February 2001 <<http://al-bab.com/saudi-internet-rules-2001>> accessed November 2016.

<sup>1718</sup> Telecom Act 2001 Issued under the Council of Ministers Resolution No. (74) dated 05/03/1422H (corresponding to 27/05/2001) Articles 37 and 38.

<sup>1719</sup> Communications and Information Technology Commission *Annual Report 2014*, 37 <<http://www.citc.gov.sa/en/MediaCenter/Annualreport/Pages/default.aspx>> accessed November 2016.

publicly available list of websites blocked by the CITC, in order to evaluate whether the remaining 15% of websites have been filtered because of their terrorist links<sup>1720</sup> and whether this has been effectively used to prevent solicitation of donations through websites. It therefore seems apparent that Saudi Arabia does not often use its Internet filtration technology to necessarily block websites which directly solicit donations for terrorist organisations, limiting the effectiveness of Saudi Arabia to control this type of Internet usage by terrorists.

Saudi Arabia's subjective website control has been severely criticised, with the UN's Economic and Social Commission for Western Asia stating in 2007 that it and other countries lacked "*the adequate regulation to ensure a censorship level that does not contradict internationally recognised rules on freedom of expression*".<sup>1721</sup> The close links between the CITU and the Saudi Government and Royal Family also provides a subjective tool which could potentially be used for suppression. For example, the Saudi Anti-Cyber Crime Law of 2007 makes it a criminal offence to "*defame or harm individuals and the development of websites that violate Saudi laws or Islamic values or that serve terrorist organisations*".<sup>1722</sup> Under the Law, those who publicise or construct websites that "*facilitate communications with [terrorist] organisations, finance them [etc.]*"<sup>1723</sup> are subject to imprisonment of up to 10 years and a fine of up to SR5million.<sup>1724</sup> Clearly, while potentially being very effective, when coupled with

---

<sup>1720</sup> Freedom House *Freedom on the Net: Saudi Arabia* (2015) <<https://freedomhouse.org/report/freedom-net/2015/saudi-arabia>> accessed November 2016.

<sup>1721</sup> United Nations Economic and Social Commission for Western Asia E/ESCWA/ICTD/2007/8 *Models for Cyber legislation in ESCWA Member Countries* (27 June 2007), 18-19 <<https://www.unescwa.org/publications/models-cyber-legislation-escwa-member-countries>> accessed April 2018.

<sup>1722</sup> Anti Cyber Crime Law 2007, Royal Decree No. M/17 26 March 2007; Murray, A. *Information Technology Law: The Law and Society* (3rd Edn. Oxford University Press, 2016), 83.

<sup>1723</sup> Anti Cyber Crime Law 2007, Royal Decree No. M/17 26 March 2007, Article 7(1).

<sup>1724</sup> *ibid.*

the vague definition of ‘terrorism’ under the subsequent Penal Law for Crimes of Terrorism and its Financing, which includes “*harming the reputation or status of the country*”,<sup>1725</sup> this captures an incredibly wide array of websites which may not be connected with internationally proscribed terrorist organisations or terrorism per se. For instance, it was found in 2009 that the SmartFilter censorship tool used by Saudi authorities had blocked several opposition websites which had shown other forms of religion<sup>1726</sup> and Saudi political reformists.<sup>1727</sup> This action is well within the confines of the Saudi Constitution, as Article 39 states that information, “*publication and all other media shall employ courteous language and the state’s regulations and they shall contribute to the education of the nation and the bolstering of its unity*” and calls for the prohibition of acts that “*foster sedition or division or harm*”.<sup>1728</sup> Yet the case of *Raif Badawi*, an Internet blogger who was arrested in 2012 on the basis of “*insulting Islam through electronic channels*”<sup>1729</sup> after he set up a website which declared a day for Saudi liberals, in order to open up discussion,<sup>1730</sup> highlights the lengths to which Saudi authorities will punish those who are freely expressing their opinions. Badawi was later sentenced to 10 years’ imprisonment, 1,000 lashes and a fine of SR1million after he appealed his initial sentence.<sup>1731</sup> This case has garnered significant international attention, with Amnesty International, whose website is still banned in Saudi

---

<sup>1725</sup> Penal Law for Crimes of Terrorism and its Financing 2013 Royal Decree No. M/16 of 27 December 2013, Article 1(1).

<sup>1726</sup> E.g. Minority Shia Groups and the Secularization of the Islamic Society. Opennet Initiative *Saudi Arabia* (6 August 2009) <<https://opennet.net/research/profiles/saudi-arabia>> accessed November 2016.

<sup>1727</sup> E.g. Voice of Saudi Women was blocked in 2008 and free speech advocates such as the Free Speech Coalition and the Saudi Human Rights Center were also blocked; *ibid*.

<sup>1728</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 41, <[http://www.parliament.am/library/sahmanadrutyunner/Saudi\\_Arabia.pdf](http://www.parliament.am/library/sahmanadrutyunner/Saudi_Arabia.pdf)> accessed 12 April 2018.

<sup>1729</sup> Human Rights Watch *Saudi Arabia: Website Editor Facing Death Penalty* (22 December 2012) <<https://www.hrw.org/news/2012/12/22/saudi-arabia-website-editor-facing-death-penalty>> accessed November 2016.

<sup>1730</sup> *ibid*.

<sup>1731</sup> Jamjoon, M. (CNN, 8 May 2014) *Saudi activist sentenced to 10 years, 1,000 lashes for insulting Islam* <<http://edition.cnn.com/2014/05/07/world/meast/saudi-activist-sentenced/>> accessed November



Arabia, stating “*Raif should never have been imprisoned in the first place*”<sup>1732</sup> and campaigning to quash his conviction.<sup>1733</sup> In 2016, the United Nations Human Rights Council also issued a warning note to those regimes with excessive Internet surveillance and website monitoring tools, by introducing a resolution which noted that the Council “[c]ondemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law”.<sup>1734</sup> Although this Resolution is non-binding, such statements could have an impact on the use of Internet filtration techniques by Saudi Arabia in the future, and have an impact on its relationships with other countries.

As noted within chapter one,<sup>1735</sup> the test of appropriateness with Saudi Arabia is lower; by virtue of the fact that it has not incorporated international human rights, including freedom of expression.<sup>1736</sup> It has also acted legally within the sovereign boundaries of its Constitution and Shari’ah, in accordance with Article 2(1) of the UN Charter.<sup>1737</sup> However, the transference of *lèse majesté* laws onto Internet communications may be an anathema for other jurisdictions such as the US and the UK, who could potentially refuse to provide mutual legal assistance to Saudi Arabia, as well as refuse extraditions, under Articles 15 and 17 of the 1999 Convention. Badawi, in his

---

2016. BBC News (19 October 2016) *Saudi blogger Raif Badawi 'faces new round of lashes'* <<http://www.bbc.co.uk/news/world-middle-east-37703312>> accessed November 2016.

<sup>1732</sup> Amnesty International *Raif Badawi* <<https://www.amnesty.org.uk/issues/Raif-Badawi>> accessed November 2016.

<sup>1733</sup> *ibid.*

<sup>1734</sup> A/HRC/32/L.20 The promotion, protection and enjoyment of human rights on the Internet (27 June 2016) Article 10.

<sup>1735</sup> Chapter 1.4.2.2.

<sup>1736</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A), Article 19.

<sup>1737</sup> Article 2(1) states that the UN “*is based on the principle of the sovereign equality of all its Members.*” Consequently, the retention of a Member State’s sovereignty is key to the co-operation principles of the UN - see *Charter of the United Nations*, <<http://www.un.org/en/charter-united-nations/index.html>> accessed November 2016.

opposition to the Saudi administration, could be considered to fall within the categories outlined in Article 15 and, had information about him been asked for from another country, this could have been refused on the basis that it would be made for the purpose of prosecuting him.<sup>1738</sup> As a result, while Saudi Arabia may be acting appropriately within its own remit and towards its own citizens, the potential harm its position could create in terms of international co-operation towards counter-terrorist financing means it could be inappropriate here.

### **6.2.2 Electronic Communications**

The measures Saudi Arabia uses to tackle terrorist websites extends to the content of emails and the use of social media in the region. The awareness of Saudi authorities of ISIL's use of social media to solicit donations is not to be underestimated, as in 2015, it was found that they had tricked potential ISIL donors through social media, such as Twitter, and had subsequently frozen 61 bank accounts.<sup>1739</sup> Consequently, Saudi Arabia has become more technology aware, and able to outsmart modern terrorist use of the Internet.

The Saudi Constitution does have provisions on privacy, under Article 41, which notes that “[t]elegraphic, postal, telephone, and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or listened to

---

<sup>1738</sup> Article 15 of the 1999 Convention for the Suppression of the Financing of Terrorism states: *Nothing in this Convention shall be interpreted as imposing an obligation to extradite or to afford mutual legal assistance, if the requested State Party has substantial grounds for believing that the request for extradition for offences set forth in article 2 or for mutual legal assistance with respect to such offences has been made for the purpose of prosecuting or punishing a person on account of that person's race, religion, nationality, ethnic origin or political opinion or that compliance with the request would cause prejudice to that person's position for any of these reasons.*

<sup>1739</sup> Financial Action Task Force *Financing of the terrorist organization Islamic State in Iraq and the Levant (ISIL)* (2015), 36 <[www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf)> accessed November 2016.

*except in cases defined by statutes.*<sup>1740</sup> However, the exceptions defined by statutes are apparent when one examines the Anti-Cyber Crime Law of 2007. Although, on the surface, the Law prohibits unauthorised access to or the spying on data transmitted through an information network,<sup>1741</sup> there is no independent data controller to verify whether the ISPs or the Government itself is monitoring content. Instead, it is almost taken for granted that Saudi authorities will monitor the content of communications and mobile phone messages<sup>1742</sup> and identification is required to purchase mobile phones in the region.<sup>1743</sup> These are major steps away from the data surveillance techniques employed by the UK and the US, which can only access the non-content, or email address and subject line, of the communications. Furthermore, there is a focus on data protection in both these countries, through the Data Protection Act 1998 in the UK and the Constitution in the US, as well as the employment of independent data controllers. Therefore, while monitoring the content of communications may be an extremely effective way of tracing terrorist finances, although this author can find no evidence terrorist financiers have been caught through these means,<sup>1744</sup> and that it is within Saudi Arabia's sovereign remit to do so, privacy concerns may again hinder international relations under Article 15 of the 1999 Convention.

---

<sup>1740</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 41. <[http://www.parliament.am/library/sahmanadrutyunner/Saudi\\_Arabia.pdf](http://www.parliament.am/library/sahmanadrutyunner/Saudi_Arabia.pdf)> accessed 12 April 2018.

<sup>1741</sup> Anti Cyber Crime Law 2007, Royal Decree No. M/17 26 March 2007, Article 3(1).

<sup>1742</sup> Freedom House *Saudi Arabia Freedom on the Net 2011* <<https://freedomhouse.org/report/freedom-net/2011/saudi-arabia>> accessed November 2016; Marlinspike, M. "A Saudi Arabia Telecom's Surveillance Pitch", *Thought Crime* (blog), (13 May 2013) <<http://bit.ly/1011Ynw>> accessed November 2016.

<sup>1743</sup> *ibid.*

<sup>1744</sup> There are overall references to the arrests of those connected with ISIL between 2015 and 2016, amounting to over 1,300 Saudi individuals and 300 foreigners. *ibid* Blanchard, C. RL33533 *CRS Report to Congress Saudi Arabia: Background and U.S. Relations* (20 September 2016) 12.

Furthermore, since the Arab Spring in 2011 and the rise of ISIL, Saudi authorities have clamped down tightly on dissenting views, quickly blocking political discourse on social media sites such as Facebook, Twitter, and YouTube.<sup>1745</sup> The Anti-Cyber Crime Law 2007 has been used to prosecute those using social media as a form of dissent to the ruling Government and Royal Family under Article 6, with Article 6(1) stating that it is an offence to produce, prepare or transmit “*materials impinging on public order, religious values, public morals and privacy, through the information network or computers*”.<sup>1746</sup> While this may be effective in monitoring and shutting down ISIL’s formidable presence on social media, again the Saudi application has been proven to capture political or moral rather than terrorism-related views. For example, Loujain al-Hathloul was arrested after she demanded to be able to drive in Saudi Arabia, then charged for her political views, expressed on Twitter, and detained for 73 days,<sup>1747</sup> and in 2014, Su’ad al-Shammari, co-founder of the Saudi Arabia Liberals website, was arrested over tweets that were described as “offensive to the heritage of the prophet Mohammad”.<sup>1748</sup> She was later released,<sup>1749</sup> but not before Article 6 was internationally criticised by humanitarian organisation Human Rights Watch on the basis of vagueness and inappropriate application.<sup>1750</sup> However, as mentioned earlier,<sup>1751</sup> Article 39 of the Saudi Convention prohibits publication of opinions which

---

<sup>1745</sup> Freedom House *Freedom on the Net 2012: Saudi Arabia* <<https://freedomhouse.org/report/freedom-net/2012/saudi-arabia>> accessed November 2016.

<sup>1746</sup> Anti-Cyber Crime Law Royal Decree No. M/17 26 March 2007 Article 6(1).

<sup>1747</sup> Bager, J. (Time, 6 February 2015) *Saudi Women Right-to-Drive Activists Deploy Twitter, Face Terrorism Court* <<http://time.com/3697073/saudi-arabia-women-drive-twitter/>> accessed November 2016.

<sup>1748</sup> Al Jazeera (23 November 2014) *Saudi Arabia 'intensifies Twitter crackdown'* <<http://www.aljazeera.com/news/middleeast/2014/11/saudi-arabia-intensifies-twitter-crackdown-2014112363955848622.html>> accessed November 2016.

<sup>1749</sup> Agence France-Presse (The Guardian, 1 February 2015) *Saudi Arabia frees associate of imprisoned blogger Raif Badawi* <<https://www.theguardian.com/world/2015/feb/01/saudi-arabia-frees-raif-badawi-associate>> accessed November 2016.

<sup>1750</sup> *ibid* Al Jazeera (23 November 2014) *Saudi Arabia 'intensifies Twitter crackdown'* <<http://www.aljazeera.com/news/middleeast/2014/11/saudi-arabia-intensifies-twitter-crackdown-2014112363955848622.html>> accessed November 2016.

<sup>1751</sup> Chapter 6.2.1.

are viewed as seditious or divisive, so the Saudi authorities are working within their remit. Despite this, growing international concern on using what are national security and counter-terrorism powers to stifle dissenting views again serve to highlight potential problems with co-operation under Article 15 of the 1999 Convention.

These counter-terrorism powers extend further, as those who have been charged with such offences are often tried in closed courts. Of concern are the powers of the Al Mabathith or secret police, who have broad authority to investigate or refer on cases to closed courts cases of ‘national security’,<sup>1752</sup> under whose definition terrorism to dissent and human rights activist cases fall,<sup>1753</sup> as well as their referrals to closed terrorism courts. In 2008, the Specialized Criminal Court was formed to hear cases of terrorism, and reaffirmed in 2014<sup>1754</sup> after the passing of the Law of Terrorism Crimes and its Financing.<sup>1755</sup> This court has been previously criticised by Wilcke on the basis that trials had been held entirely in secret, with no independent observers to find out whether due process had been followed,<sup>1756</sup> in stark comparison to countries such as the US and the UK.<sup>1757</sup> Additionally, the US Department of State noted the case of Mohamed Saleh al-Bajady, a political dissident and a founding member of Saudi Civil and Political Rights Association (ACPRA),<sup>1758</sup> who was arrested for demanding political and legal reforms. During his trial, the court denied both observers

---

<sup>1752</sup> US Department of State *Saudi Arabia 2015 Human Rights*, 8 <<http://www.state.gov/documents/organization/253157.pdf>> accessed November 2016.

<sup>1753</sup> *ibid.*

<sup>1754</sup> *ibid.*

<sup>1755</sup> Law of Terrorism Crimes and its Financing Article 8.

<sup>1756</sup> Wilcke, C. *Human Rights and Saudi Arabia's Counterterrorism Response; Religious Counselling, Indefinite Detention, and Flawed Trials* (Human Rights Watch, 10 August 2009), 19-20 <<https://www.hrw.org/report/2009/08/10/human-rights-and-saudi-arabias-counterterrorism-response/religious-counseling>> accessed June 2018.

<sup>1757</sup> E.g. The Constitution of the United States 1787 enshrines the right to a speedy and public trial under the Sixth Amendment and the UK has the with to a fair trial under s.6 of the Human Rights Act 1998 c.42; Chapter 2.4.2.2.

<sup>1758</sup> US Department of State *Saudi Arabia 2015 Human Rights* 14.

and al-Bajady’s lawyer access to the courtroom.<sup>1759</sup> Although later released,<sup>1760</sup> al-Bajady’s case highlights the use of counter-terrorism powers by Saudi Arabia to block independent oversight of its judicial system. As noted earlier, the Universal Declaration of Human Rights is non-binding, however, Article 17 of the 1999 Convention is. This Article provides for those who are taken into custody or subject to proceedings under the Convention “*shall be guaranteed fair treatment, including enjoyment of all rights and guarantees in conformity with the law of the State in the territory of which that person is present and applicable provisions of international law, including international human rights law*”.<sup>1761</sup> As a result, the dependence on hearing such cases *in camera*, while within the law of the Saudi State, potentially brings Saudi Arabia into direct conflict with the Universal Declaration of Human Rights, Article 10, which states that “[e]veryone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him”.<sup>1762</sup> As Wilcke states, when courts arrive to their judgements in secret, it is hard to assess whether they have been fairly reached<sup>1763</sup> and international regulations mean that courts should only be held *in camera* in very narrow circumstances, such as the sexual abuse of a minor, or limited cases of national security,<sup>1764</sup> as happens in the UK and the US. As a result, the view that Saudi Arabian authorities have far exceeded what is required of them to prosecute potential terrorism cases, and have eventually used these powers to convict dissidents, potentially damage

---

<sup>1759</sup> *ibid.*

<sup>1760</sup> *ibid.*

<sup>1761</sup> A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999), Article 17.

<sup>1762</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A), Article 10.

<sup>1763</sup> Wilcke, C. *Human Rights and Saudi Arabia’s Counterterrorism Response; Religious Counselling, Indefinite Detention, and Flawed Trials* (Human Rights Watch, 10 August 2009), 20

<<https://www.hrw.org/report/2009/08/10/human-rights-and-saudi-arabias-counterterrorism-response/religious-counseling>> accessed June 2018.

<sup>1764</sup> *ibid.*

international mutual assistance under the 1999 Convention because some countries may view others' actions as inappropriate or breach the human rights of their subjects.

The over-use of counter-terrorism powers in this area also appears to have been exploited by ISIL, who have used social media to insult and issue threats to the Saudi Royal Family and using hashtags on Twitter such as “Saudi Arabia Executes the Honest and Righteous Religious Scholars”,<sup>1765</sup> somewhat blurring the lines between exercising freedom of speech and dissemination of extremist views. As Blanchard notes *“IS critiques of the Al Saud may have resonance among some Saudis who disagree with the government’s policies or those who have volunteered to fight in conflicts involving other Muslims over the last three decades”*.<sup>1766</sup> Furthermore, as the US Department of State outlined in 2016, *“[r]ecent regional turmoil and a sophisticated use of social media have facilitated charities outside of Saudi Arabia with ties to violent extremists to solicit donations from Saudi donors”*.<sup>1767</sup> Due to a series of terrorist attacks by ISIL in Saudi Arabia between 2014 and 2016,<sup>1768</sup> it is perhaps unsurprising that Saudi authorities have been quick to crack down on politically different views. Yet, by increasingly controlling freedom of speech and expression over the Internet, Saudi Arabia may be fuelling support for ISIL. Therefore, in order to shift the balance between effectively targeting communications to prevent solicitation of donations and

---

<sup>1765</sup> Kingdom of Saudi Arabia *The Kingdom of Saudi Arabia and Counterterrorism* (2016) 46. <<https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf>> accessed November 2016.

<sup>1766</sup> *ibid* Blanchard, C. RL33533 *CRS Report to Congress Saudi Arabia: Background and U.S. Relations* (20 September 2016) 12.

<sup>1767</sup> US Department of State *Country Reports on Terrorism 2015 Chapter 2. Country Reports: Middle East and North Africa Overview* <<http://www.state.gov/j/ct/rls/crt/2015/257517.htm>> accessed November 2016.

<sup>1768</sup> *ibid* *The Kingdom of Saudi Arabia and Counterterrorism* 49-50.

enabling genuine political or religious disagreement, Saudi Arabia must revisit its policy towards social media comment, or at the very least, make more use of the persuasive techniques of the Sakinah Campaign.<sup>1769</sup>

### **6.3. Legitimate sources of finance**

The 9/11 Commission outlined serious concerns about the vulnerability of the Saudi Arabian financial sector and the use of charitable donations by al-Qaeda and the 9/11 attackers in their quest to finance the bombings.<sup>1770</sup> Specifically, it was noted that Saudi Arabia was part of the ‘Golden Chain’ of terrorist financing,<sup>1771</sup> with lax controls over charitable donations and the infiltration of some of its biggest charities by al-Qaeda. Furthermore, financial institutions themselves came under tightened scrutiny, as there were few internationally recognised controls available to counteract financial crime.<sup>1772</sup>

#### **6.3.1. Charities**

With Islamic religious *zakat*, or charitable giving, generating approximately \$10billion per year in Saudi Arabia alone by 9/11,<sup>1773</sup> and the fact that there was “no formal

---

<sup>1769</sup> Chapter 6.2.1. *supra*.

<sup>1770</sup> *9/11 Commission Report* (22 July 2004), 371-374 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1771</sup> *ibid* 55.

<sup>1772</sup> For example, there was no application of the Vienna Convention on AML.

<sup>1773</sup> Estimated in 2002. Brisard, J.C. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing – Report Prepared for the President of the UN Security Council* (Investigative Project, 19 December 2002) <<http://www.investigativeproject.org/documents/testimony/22.pdf>> accessed November 2016.

NB. Jean Charles Brisard has been subject to a number of defamation lawsuits regarding his report e.g. *bin Mahfouz v Jean Charles Brisard* [2006] EWHC 1191 (QB); *Al-Amoudi v Brisard* [2007] 1 WLR 113.



*oversight mechanism for donations*”,<sup>1774</sup> the issue of terrorists infiltrating charities has been at the forefront of Saudi efforts to disrupt and prevent terrorist finances from being raised in this way. After 9/11, it was clear that, with over \$3-4billion being raised by Saudi charities per year and 10-20% of that figure being channelled overseas,<sup>1775</sup> some of those funds were being diverted into terrorist causes. As Levitt and Ryder note, al-Qaeda and Osama bin Laden had links with both Saudi zakat and charitable organisations,<sup>1776</sup> with Ryder quoting Raphaeli as stating that Saudi was “*unquestionably the largest cash source of cash to al-Qaeda and other terrorist organisations*”.<sup>1777</sup> Perhaps the most infamous Saudi charity to have links with al-Qaeda in the wake of 9/11 was the Al-Haramain Islamic Foundation,<sup>1778</sup> whose offices were listed as supporting al-Qaeda by the UN in 2002 for “*‘participating in the financing, planning, facilitating, preparing or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf or in support of’ Al-Qaida*” under Security Council Resolution 1267.<sup>1779</sup> Al-Haramain was a Saudi-based Non-Governmental Organisation (NGO), which had offices based throughout the world. It was

---

<sup>1774</sup> 9/11 Commission Report (22 July 2004), 372 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1775</sup> *ibid* Brisard, J.C. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing – Report Prepared for the President of the UN Security Council* (Investigative Project, 19 December 2002) <<http://www.investigativeproject.org/documents/testimony/22.pdf>> accessed November 2016, 26; *ibid* Prados, A.B. & Blanchard, C.M. RL32499 CRS Report to Congress – *Saudi Arabia: Terrorist Financing Issues* (8 December 2004, updated 14 September 2007), 15.

<sup>1776</sup> Levitt, M.A. *The Political Economy of Middle East Terrorism* (Washington Institute, December 2002) 6(4) Middle East Review of International Affairs 10; Ryder, N. *A False Sense of Security? An analysis of Legislative Approaches Towards to Prevention of Terrorist Finance in the United States and the United Kingdom* (2007) J.B.L. Nov 821, 840.

<sup>1777</sup> *ibid* Ryder N. *A False Sense of Security? An analysis of Legislative Approaches Towards to Prevention of Terrorist Finance in the United States and the United Kingdom* (2007) J.B.L. Nov 821, 840; Raphaeli, N. *Financing of terrorism: sources, methods, and channels* (2003) 15(4) *Terrorism and Political Violence* 59, 77.

<sup>1778</sup> *ibid*; 9/11 Commission Report (22 July 2004), 170-171 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1779</sup> United Nations Security Council *Narrative Summaries and Reasons for Listing QDe.071 AL-HARAMAIN ISLAMIC FOUNDATION (BOSNIA AND HERZEGOVINA)* <[https://www.un.org/sc/suborg/en/sanctions/1267/qa\\_sanctions\\_list/summaries/entity/al-haramain-islamic-foundation-\(bosnia-and-herzegovina\)](https://www.un.org/sc/suborg/en/sanctions/1267/qa_sanctions_list/summaries/entity/al-haramain-islamic-foundation-(bosnia-and-herzegovina))> accessed November 2016.

subsequently found after 9/11 that Al-Haramain's Bosnia and Herzegovina office had been financing al-Qaeda,<sup>1780</sup> and had links to an Egyptian terrorist group, Al-Gama'at al-Islamiyya,<sup>1781</sup> although US authorities had apparently raised concerns about its links with Saudi officials since 1998.<sup>1782</sup> It was not until 2002 that Saudi, in joint efforts with the United States, designated this charity.<sup>1783</sup> As Brisard explained in 2002, many of the terrorist funds channelled through these organisations were as a result of Saudi Arabia's "*soft regulations*".<sup>1784</sup> Consequently, Saudi Arabia has since toughened its stance on charitable organisations.

For example, Saudi Arabia froze all charitable assets of charities acting outside the Kingdom, ensuring that they could not access their bank accounts without special permission.<sup>1785</sup> Saudi law also decreed that charities could not collect in public places or mosques,<sup>1786</sup> and a National Commission for Charities Abroad was proposed to monitor charitable donations and prevent their use in terrorism.<sup>1787</sup> Saudi laws have become even more restrictive towards charitable finances since, preventing ATM or

---

<sup>1780</sup> *ibid*; 9/11 Commission Report (22 July 2004), 170 <<http://www.9-11commission.gov/>> accessed November 2016.

<sup>1781</sup> *ibid*.

<sup>1782</sup> Roth, J. Greenberg, D. Wille, S. *National Commission on Terrorist Attacks Upon the United States Staff Monograph on Terrorist Financing* (2004), 12.

<sup>1783</sup> Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008), 126.

<sup>1784</sup> Brisard, J.C. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing – Report Prepared for the President of the UN Security Council* (Investigative Project, 19 December 2002), 22 <<http://www.investigativeproject.org/documents/testimony/22.pdf>> accessed November 2016.

<sup>1785</sup> Cordesman, A. *Saudi Arabia: Friend or Foe in the War on Terror?* (2006) 8(1) Middle East Policy 28, 34.

<sup>1786</sup> *ibid*.

<sup>1787</sup> *ibid*; *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues* (8 December 2004, updated 14 September 2007) 16-17.

credit cards from being issued to charitable accounts,<sup>1788</sup> with a mandatory single-disbursement bank account<sup>1789</sup> and an approved official with signatory authority to ensure a tighter control over funds.<sup>1790</sup> This goes further than those provisions outlined by the US and the UK, demonstrating Saudi's commitment to tightening controls over charitable giving. Furthermore, donations to charities being diverted to causes other than authentic humanitarian organisations are now outlawed,<sup>1791</sup> with the transfer of funds by charities to any organisation or person outside Saudi Arabia, without government approval being prohibited,<sup>1792</sup> capturing those charities which work online or outside of the Kingdom's control. Furthermore, the financial information of Saudi charities is entered into a database by the Ministry of Labour and Social Affairs, with quarterly updates, which is integrating this information with charities registered with the Ministry of Islamic Affairs.<sup>1793</sup> However, the effectiveness of these provisions still remains debatable. As noted in 6.2.1., the Saudi Al-Quds Intifada Committee website maintained records of financial support given to families of Palestinians killed in the Israel-Palestine conflict, including records of 60 notorious suicide bombers and militants,<sup>1794</sup> only being removed in 2005.<sup>1795</sup> Consequently, the commitment of

---

<sup>1788</sup> Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008), 121-122.

<sup>1789</sup> *ibid.*

<sup>1790</sup> *ibid.*

<sup>1791</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010), 168, para. 783 <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016.

<sup>1792</sup> Royal Decree No.2/1 dated 6/1/1425 AH, Article 6; Domestic Saudi Commission for Rescue and Charity Abroad.

<sup>1793</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010), 168, para. 782 <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016; Kingdom of Saudi Arabia *The Kingdom of Saudi Arabia and Counterterrorism* (2016) 26. <<https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf>> accessed November 2016.

<sup>1794</sup> *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues*, 15 (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

<sup>1795</sup> *ibid* 16.

Saudi Arabia in counteracting the use of terrorist finances in this manner has been argued as questionable. Allegations have also been raised of close links between the Saudi Government with terrorist-affiliated charities through investigations of the Shaykh Sulayman Abd al-Aziz al-Rajhi Foundation (SAAR)<sup>1796</sup> and the Saudi High Commission Aid for Bosnia,<sup>1797</sup> both of which were suspected of providing assistance for militants and terrorist organisations, such as HAMAS and al-Qaeda.<sup>1798</sup> As Levitt claims, the Saudi Government also indirectly financed organisations such as the International Islamic Relief Organisation through its Muslim World League charity.<sup>1799</sup> Furthermore, despite introducing AML/CTF Suspicious Activity Reports (SARs) for charities in 2003,<sup>1800</sup> these were not sent to the Saudi Arabian Financial Investigation Unit (SAFIU), but instead to the Ministry of Labour and Social Affairs (MOSA), leaving them outside the same legal framework as Suspicious Transaction Reports under the Anti-Money Laundering Law.<sup>1801</sup> In 2010, the MENAFATF found that no SARs has been filed with MOSA or SAFIU,<sup>1802</sup> and that no MOSA staff had filed SARs on any charity.<sup>1803</sup> It therefore appeared that after 9/11, the Saudi Government, whether through its indirect involvement with terrorist-affiliated charities or not, had little oversight of its charities, with this ineffectiveness compounded by the lack of an independent authority to monitor their transparency and the use of their funds – contrasting sharply with the actions of the US and the UK.

---

<sup>1796</sup> *ibid* Levitt, M. 10.

<sup>1797</sup> *ibid* 8.

<sup>1798</sup> *ibid* 6.

<sup>1799</sup> *ibid* 7-8.

<sup>1800</sup> Ministry of Social Affairs Circular No. 41735, dated 22/9/1424H.

<sup>1801</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010), 169, para.784 <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016.

<sup>1802</sup> *ibid* para. 785.

<sup>1803</sup> *ibid*.

Moreover, the stringent use of AML/CTF provisions on charities and preventing them from operating abroad surely raises the same concerns as outlined in chapters four and five about the ability of humanitarian charities to deliver their aid abroad.<sup>1804</sup> While there is no specific evidence of inappropriate use of these provisions in Saudi Arabia, it does not mean that legitimate charities would find it easy to access finances if a bank decided to freeze much-needed assets. One can only surmise, however, that much of the difficulties would be the same with Saudi Arabian charities, who are currently limited to working within the Kingdom.

### **6.3.2. Financial Institutions**

Again, Saudi Arabia has been the focus of international efforts on channelling finances through financial institutions in the wake of 9/11, due to alleged links of Saudi non-profit organisations with, in particular, Arab Bank plc. in the Hashemite Kingdom of Jordan. Arab Bank is alleged to have funnelled money to Iran, Syria and HAMAS,<sup>1805</sup> extending its operations internationally.<sup>1806</sup> It has also been argued in *Linde*<sup>1807</sup> and *Almog*<sup>1808</sup> that there was alleged involvement of Saudi Arabia's charities, such as the Al Quds Intifada Committee, with banks accused of aiding terrorist financing.<sup>1809</sup> Both cases share remarkable parallels with HSBC's hiding of money laundering and

---

<sup>1804</sup> See Chapter four, 4.3.1. and chapter five, 5.3.1. for further information.

<sup>1805</sup> *ibid* Levitt, M. 3.

<sup>1806</sup> *ibid* 4.

<sup>1807</sup> *Linde et al. v. Arab Bank PLC* (2004) 04 CV 02799 (E.D.N.Y. filed 2 July 2004); Discovery Order sought before trial – 384 F. Supp. 2d 571 (E.D.N.Y. 2005) and granted 2006 WL 3422227 (E.D.N.Y. 25 November 2006).

<sup>1808</sup> *Almog v. Arab Bank PLC* 471 F. Supp. 2d 257, 285 (E.D.N.Y. 2007).

<sup>1809</sup> *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues*, 5-6 (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

terrorist financing around the same time.<sup>1810</sup> In addition, the hawala system of informal value transfer complicated Saudi banking arrangements, due to its traditional lack of record-keeping.<sup>1811</sup> Clearly, there was a lack of openness and transparency within the Saudi system of banking, which terrorists used their advantage. Since 2003, Saudi Arabia has approved several pieces of legislation, including the Anti-Money Laundering Law,<sup>1812</sup> requiring financial institutions to keep records of transactions for up to ten years,<sup>1813</sup> the strict enforcement of ‘know your customer’ (KYC) rules<sup>1814</sup> and announcing the SAFIU as part of the Saudi Arabian Monetary Authority (SAMA) to monitor transactions.<sup>1815</sup> Additionally, unlicensed alternative remittance services such as hawala are illegal.<sup>1816</sup> Finally, Saudi Arabia has become an observer country under the Financial Action Task Force’s (FATF) Recommendations, with a view to becoming a full member of the FATF in due course.<sup>1817</sup> Therefore, Saudi Arabia has a number of instruments which have the potential to enhance the effectiveness of its CTF provisions and is aiming to become fully compliant with FATF Recommendations.

---

<sup>1810</sup> Chapter five, 5.3.2.

<sup>1811</sup> Perkel, W. *Money Laundering and Terrorism: Informal Value Transfer Systems* (2004) 41 *American Criminal Law Review* 183; Pathak, R. *The obstacles to regulating the hawala: a cultural norm or a terrorist hotbed?* (2003) 27 *Fordham Int'l L.J.* 2007.

<sup>1812</sup> Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003.

<sup>1813</sup> *ibid* Article 5.

<sup>1814</sup> Saudi Arabian Monetary Authority *Rules Governing the Opening of Bank Accounts* (2003; fourth update 2012) [http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules\\_Governing\\_the\\_Opening\\_of\\_Bank\\_Accounts\\_ver4.pdf](http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules_Governing_the_Opening_of_Bank_Accounts_ver4.pdf) accessed June 2018 Title III: Procedural Rules, Rule 100; Cordesman, A. *Saudi Arabia: Friend or Foe in the War on Terror?* (2006) 8(1) *Middle East Policy* 28, 33.

<sup>1815</sup> *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues*, 24 (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

<sup>1816</sup> SAMA’s rules governing licensing were updated in 2015; Saudi Arabian Monetary Authority *Rules Governing Money Changing Business Issued by Decision of the Minister of Finance No. 1357 dated 01/05/1432H* <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p\\_SortBehavior=0&p\\_SAMAFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p_SortBehavior=0&p_SAMAFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed November 2016.

<sup>1817</sup> Saudi Arabian Monetary Authority *The Kingdom of Saudi Arabia’s Accession to Observer Member in FATF* (2 August 2015) <<http://www.sama.gov.sa/en-US/News/Pages/News08022015.aspx>> accessed November 2016.

Nevertheless, as mentioned under 6.2.1., the AML/CTF offences were not separated, nor were they linked fully with UN Security Council Resolutions, severely hampering financial institutions' efforts in tracing and preventing the flow of terrorist financing through the financial system. This can be seen through the asset freezing regime of Saudi Arabia immediately after 9/11. Compared with the UK, which was found in *Ahmed* to have taken its asset-freezing regime beyond what was necessary,<sup>1818</sup> the MENAFATF Mutual Evaluation Report of Saudi Arabia highlighted that there was a large gap in the freezing and disrupting terrorist finances. Freezing orders in Saudi Arabia were only applied under UN Resolution 1267 and not inclusive of Resolution 1373, meaning that there was only a focus on Taliban or al-Qaeda related assets, rather than terrorist financing as a whole.<sup>1819</sup> As the Report further explained, the Royal Order S/2496 of 19 March 2003, which was the 'backbone' of the CTF freezing regime in Saudi Arabia,<sup>1820</sup> directed relevant authorities to "*freeze all funds or other assets of any individual or entities listed on the lists issued by the UN and not to restrict the freezing to bank accounts only*",<sup>1821</sup> but did not mention Resolution 1373 in any capacity.<sup>1822</sup> Furthermore, MENAFATF had found that some authorities had "*indicated that lists of terrorists based on UNSCR 1373 had to be dealt with in*

---

<sup>1818</sup> *HM Treasury v Mohammed Jabar Ahmed and others; Her Majesty's Treasury v Mohammed al-Ghabra; R (on the application of Hani El Sayed Sabaei Youssef) v Her Majesty's Treasury* [2010] UKSC 2.

<sup>1819</sup> For example, Article 1(c) Resolution S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts states that assets of *persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts* and Article 4(b) of Resolution S/RES/1267 (1999) on Afghanistan stated that *funds and other financial resources, including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by the Taliban* should be frozen.

<sup>1820</sup> Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010), 182, para. 43 <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016.

<sup>1821</sup> *ibid.*

<sup>1822</sup> *ibid.*

*the same way as UNSCR 1267*”,<sup>1823</sup> yet Resolution 1373 does not have a list of designated entities.<sup>1824</sup> Therefore, while Saudi Arabian banks had frozen 94 accounts and seized banking assets totalled \$6million,<sup>1825</sup> the effectiveness of such provisions between 2003 and 2010 were on the basis of a partial application of international guidelines, limiting Saudi effectiveness in this area.

Since then, Saudi Arabia has ‘*set the legal basis*’<sup>1826</sup> for implementing Resolution 1373 under Article 32 of the Law Countering Terrorism Crimes and its Financing, by establishing the mechanisms for implementing its requirements through the Permanent Committee on Combating Terrorism.<sup>1827</sup> Furthermore, this mechanism was developed under Royal Order No. 25505 dated 14 April 2012,<sup>1828</sup> through which competent authorities<sup>1829</sup> “*shall prohibit and cease financing terrorist acts; and freeze without delay funds and any assets or economic resources owned by persons who commit, try to commit, participate in or facilitate terrorist acts*”,<sup>1830</sup> closely reflecting the wording of Resolution 1373. However, it remains to be seen whether Saudi is able to effectively use this power, as the statistics the last MENAFATF Follow up Report used only went up to 2013, when the Law of Terrorism Crimes and Financing was first introduced. Therefore, the ability of Saudi banks to freeze ISIL funds is yet to be included, and it is difficult to assess whether these changes have been effective in comparison with the UK and the US, which have implemented asset freezing measures under Resolution 1373 since 2001.

---

<sup>1823</sup> *ibid* 183.

<sup>1824</sup> *ibid*.

<sup>1825</sup> *ibid* 196, para. 49.

<sup>1826</sup> MENAFATF *Mutual Evaluation Report 4th Follow-Up Report for Saudi Arabia* (17 June 2014), 72, 24 <[http://www.menafatf.org/sites/default/files/KSA\\_Exit\\_report\\_EN.pdf](http://www.menafatf.org/sites/default/files/KSA_Exit_report_EN.pdf)> accessed June 2018.

<sup>1827</sup> *ibid*.

<sup>1828</sup> *ibid*.

<sup>1829</sup> E.g. Ministry of the Interior, Ministry of Justice, Ministry of Finance, Ministry of Commerce and Industry, SAMA, and financial institutions – *ibid* 74, 24.

<sup>1830</sup> *ibid* 74, 24.



Furthermore, the KYC guidelines employed by financial institutions have previously been criticised as being ‘insufficient’,<sup>1831</sup> showing that Saudi financial institutions needed to increase the amount of customer information they collected. This is imperative when dealing with Internet customers, as customers are not necessarily going to open their accounts face-to-face. Under Article 4 of the Anti-Money Laundering Law 2003, “[t]he identity of the clients shall be verified according to official documents, at the initiation of dealing with the clients”.<sup>1832</sup> This meant, ostensibly, that customers would have to bring the relevant documentation in order to be able to open an account. Although there are further guidelines to dealing with online customers under SAMA’s rules,<sup>1833</sup> which include Customer Due Diligence (CDD), such as no account could be opened for new customers without interviewing them,<sup>1834</sup> and that phone and online banking could only be provided to existing customers,<sup>1835</sup> MENAFATF found in 2010 that the Internet Banking Guidelines in 2001 did not address AML/CTF risks.<sup>1836</sup> Despite user protection procedures, the Report found that there was “no information pertaining to the extent/validity/effectiveness of measures undertaken by financial institutions to prevent the misuse of new technologies for ML and TF purposes”.<sup>1837</sup> Furthermore, the CDD rules, when applied to existing customers, who were already granted online banking and electronic transfer services, were

---

<sup>1831</sup> *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues*, 24 (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

<sup>1832</sup> Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003, Article 4.

<sup>1833</sup> Rule 100(8), Title III Procedural Rules Saudi Arabian Monetary Authority *Rules Governing the Opening of Bank Accounts* (2003; fourth update 2012) <[http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules Governing the Opening of Bank Accounts ver4.pdf](http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules%20Governing%20the%20Opening%20of%20Bank%20Accounts%20ver4.pdf)> accessed June 2018.

<sup>1834</sup> *ibid*.

<sup>1835</sup> Article 5.1.5 SAMA Rules Governing Anti-Money Laundering & Combating Terrorist Financing; Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010), 93 para. 446; 94 para. 452 <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016.

<sup>1836</sup> *ibid* 94, para. 449.

<sup>1837</sup> *ibid* 94, para. 450.

found by MENAFATF not to have been enhanced in comparison with new customers,<sup>1838</sup> and that sanctions for poor implementation were missing.<sup>1839</sup> Consequently, the MENAFATF Report drew the conclusion that effectiveness of these provisions were ‘questionable’.<sup>1840</sup>

This still creates a subsequent query as to the effective implementation of Saudi legislation when it is applied to non-face-to-face transactions over the Internet, whereby, as outlined in chapters four and five, more stringent identification measures are needed, including a risk-based approach.<sup>1841</sup> The follow-up Report by MENAFATF does not mention updates on non-face-to-face transactions specifically, however, it outlines that both Article 5 of the Anti-Money Laundering Law and Article 39 of the Law of Terrorism Crimes and Financing require financial institutions to continuously verify the identity of the involved parties based on official documents.<sup>1842</sup> Furthermore, the SAMA Rules Governing Anti-Money Laundering & Combating Terrorist Financing<sup>1843</sup> adopts a risk-based approach to CDD,<sup>1844</sup> and notes that “*banks and money exchangers should be required to have policies in place and take such measures as may be needed to prevent the misuse of technological developments*”,<sup>1845</sup>

---

<sup>1838</sup> *ibid.*

<sup>1839</sup> *ibid.*

<sup>1840</sup> *ibid.*

<sup>1841</sup> Chapter four, 4.3.2. and chapter five, 5.3.2.

<sup>1842</sup> MENAFATF *Mutual Evaluation Report 4th Follow-Up Report for Saudi Arabia* (17 June 2014) 28, 9 <[http://www.menafatf.org/sites/default/files/KSA\\_Exit\\_report\\_EN.pdf](http://www.menafatf.org/sites/default/files/KSA_Exit_report_EN.pdf)> accessed June 2018.

<sup>1843</sup> Saudi Arabian Monetary Authority *Rules Governing Anti-Money Laundering & Combating Terrorist Financing Third Update, 2012* <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p\\_SortBehavior=0&p\\_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p_SortBehavior=0&p_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed November 2016.

<sup>1844</sup> *ibid* Rule 4.1.

<sup>1845</sup> *ibid* Rule 5.1.5.

with these institutions applying, at a minimum, SAMA's Rules on Electronic Banking.<sup>1846</sup> Yet, despite these improvements to the overarching legal framework, the effectiveness of these provisions are also difficult to gauge as there is little information provided by the Saudi Government regarding the enforcement of its CTF provisions.<sup>1847</sup> Without knowing how the full financial or identification details of customers is applied, the effectiveness of finding terrorist finances in traditional, let alone online, banking is severely compromised, as there is no measure of success or failure.

Moreover, although the Anti-Money Laundering Law and SAMA's Rules provide a system of Suspicious Transaction Reports (STRs) on transactions,<sup>1848</sup> it was found in 2007 that updated declaration forms needed to report suspicious transactions under the Act had not yet been issued,<sup>1849</sup> reducing any assistance reporting requirements could give in finding terrorist finances channelled through formal financial systems. The MENAFATF in 2010 further found that the SAFIU only received 1,019 STRs by 2008 and, of these, 769 were from financial institutions.<sup>1850</sup> Furthermore, the amount of STRs disseminated to the Secret Police/ Al-Mabahith for CTF investigation purposes in 2008 was just 18.<sup>1851</sup> Consequently, the Report stated that “[t]he numbers of STRs and disseminations seem low, taking into account the size of the

---

<sup>1846</sup> *ibid.*

<sup>1847</sup> E.g. The last MENAFATF Mutual Evaluation Report Follow up was in 2014.

<sup>1848</sup> Under Article 8. The Law also set up the SAFIU under Article 11. Under Saudi Arabian Monetary Authority Rules Governing Anti-Money Laundering & Combating Terrorist Financing Third Update, 2012 Rule 4.8.1. <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&&p\\_SortBehavior=0&p\\_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&&p_SortBehavior=0&p_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed November 2016.

<sup>1849</sup> *ibid* Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues*, 26-27 (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018.

<sup>1850</sup> MENAFATF Mutual Evaluation Report 2010, [214, 215], 52, 53.

<sup>1851</sup> *ibid* 55-56, para 224.

*population, the very large numbers of visitors (mainly pilgrims), the size of the remittance sector (the second largest in the world), the number of reporting entities and more particularly the large number of FIs*".<sup>1852</sup> By 2014, SAFIU's Annual Report noted that 2240 AML STRs were submitted and, of these 1967 were from financial institutions.<sup>1853</sup> Yet, by comparison, just 126 terrorist financing STRs were submitted, with 37 being passed on for further investigation.<sup>1854</sup> Again, these figures seem startlingly low for a country with a population of 28 million<sup>1855</sup> and, when comparing the UK's Suspicious Activity Reports (SARs) from the same period, 354,186<sup>1856</sup> and of these 1,342 were disseminated to the UK National Terrorist Financial Investigation Unit,<sup>1857</sup> these figures show that Saudi Arabian financial institutions are still under-reporting terrorist financing. This is also true when comparing the US's Financial Intelligence Unit, FinCEN's, SARs from the same period, with 1,659,119 were filed from all institutions,<sup>1858</sup> and of these, 1,295 were highlighted as having connections with terrorist financing.<sup>1859</sup> SAFIU's figures also represents a drop from a high of 217 terrorist financing STRs in 2012,<sup>1860</sup> leading to questions about the capability of Saudi financial institutions to cope with rising finances from ISIL being channelled through their banks since 2012, as well as those suspicious transactions being generated from online transactions. It is therefore questionable whether the STRs have been used

---

<sup>1852</sup> *ibid* 249, 60.

<sup>1853</sup> Saudi Arabia Financial Intelligence Unit *Annual Report 2014* (Ministry of the Interior), 18 <<https://www.moi.gov.sa/wps/portal/Home/sectors/safiu>> accessed November 2016.

<sup>1854</sup> *ibid* 22.

<sup>1855</sup> Central Intelligence Agency *World Fact Book: Saudi Arabia* (2016). <<https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html>> accessed November 2016.

<sup>1856</sup> National Crime Agency *Suspicious Activity Reports (SARs) Annual Report 2014*, 7 <<http://www.nationalcrimeagency.gov.uk/publications/464-2014-sars-annual-report>> accessed November 2016.

<sup>1857</sup> *ibid* 32.

<sup>1858</sup> FinCEN *SAR Stats* <[https://www.fincen.gov/news-room/sar-technical-bulletins?field\\_date\\_release\\_value=&field\\_date\\_release\\_value\\_1=&field\\_tags\\_sar\\_report\\_target\\_id=687](https://www.fincen.gov/news-room/sar-technical-bulletins?field_date_release_value=&field_date_release_value_1=&field_tags_sar_report_target_id=687)> accessed April 2018.

<sup>1859</sup> *ibid*.

<sup>1860</sup> *ibid* SAMA Annual Report 24.

effectively and whether financial institutions have been provided with the proper training or have sufficient penalties if they do not apply them.

Again, the lack of a legal framework to apply data protection rules would be of concern with regard to the appropriateness of how far Saudi authorities take their reporting mechanisms. Although Shari'ah principles respect the right of privacy and prohibit spying,<sup>1861</sup> replicated in the Basic Law of Governance 1992, which protects the privacy of individuals<sup>1862</sup> and there are provisions under the Anti-Cyber Crime Law to prevent unauthorised access to banking information,<sup>1863</sup> there is nothing to suggest that law enforcement authorities could obtain financial records. By comparison, the US, which uses the Right to Financial Privacy Act of 1978<sup>1864</sup> to limit government access to subpoenas and warrants,<sup>1865</sup> and the USA PATRIOT Act of 2001 to list specific offences where government access is allowed,<sup>1866</sup> Article 8 of the Anti-Money Laundering Law only specifies that documents shall be submitted “*upon request*”.<sup>1867</sup> It therefore does not refer back to confidentiality, unlike the Law of Terrorism Crimes and its Financing, which notes that “[a]ny information disclosed by financial institutions... may be exchanged with specialized authorities in the Kingdom after adequately ensuring confidentiality. Authorities may only disclose the information necessary for use in an investigation or lawsuit related to the crime of funding terrorism”.<sup>1868</sup> As noted above, however, Article 41 of the Saudi Constitution does

---

<sup>1861</sup> 49:12 Qur'an: *O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of repentance and Merciful* The Holy Qura'n <<https://www.alislam.org/quran/>> accessed June 2018.

<sup>1862</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 17.

<sup>1863</sup> Article 4(2) Anti-Cyber Crime Law 2007.

<sup>1864</sup> The Right to Financial Privacy Act of 1978 (Pub. L. 95-630, 92 Stat. 3461) 12 U.S.C. 35, §3401.

<sup>1865</sup> *ibid* §3405, §3406.

<sup>1866</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 167.

<sup>1867</sup> Anti-Money Laundering Law 2003, Article 8.

<sup>1868</sup> Law of Terrorism Crimes and its Financing 2013, Article 39.

have exemptions to the overall notion of privacy, which the Law adheres to. Consequently, while Saudi Arabia is moving in the right direction to balance the effectiveness of using financial records in CTF investigations with confidentiality, there is still the absence of an independent data controller, which could help in providing relevant legal arguments and training for financial institutions and Government agencies to ensure that confidentiality is maintained, unless a case is fully investigated.

#### **6.4 Cybercrime**

With over 6.5 million or 58% of its online users suffering from cybercrime in 2015,<sup>1869</sup> nearly ten percent above the global average,<sup>1870</sup> Saudi Arabia suffers from substantial vulnerability in tackling cybercrime. Furthermore, by 2008, Saudi Arabia was ranked as the leading country in the region as the target and source of malicious activities online.<sup>1871</sup> Saudi Arabia has acted only relatively recently against using the Internet for cybercrime and its subsequent use in terrorist financing. For example, in 2007, it introduced its Anti-Cyber Crime Law, criminalising unlawful access to computers<sup>1872</sup> and, as mentioned earlier, levying considerable penalties against those who use websites to finance terrorism.<sup>1873</sup> Furthermore, the Electronic Transactions Law of 2007<sup>1874</sup> sets out to prevent the misuse of and fraud in electronic transactions.<sup>1875</sup> Yet, there are a number of issues surrounding the application of such legislation and whether they are effective in combating cybercrime. It is necessary also to outline

---

<sup>1869</sup> Arab News *Cybercrime hit 6.5m in Kingdom last year* (11 August 2016) <<http://www.arab-news.com/node/967966/saudi-arabia>> accessed November 2016.

<sup>1870</sup> *ibid.*

<sup>1871</sup> El-Guindy, M. *Cybercrime in the Middle East* (ISSA Journal, 2008) <<http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf>> accessed November 2016.

<sup>1872</sup> Anti-Cyber Crime Law of 2007 Article 3(2).

<sup>1873</sup> *ibid* Article 7.

<sup>1874</sup> Electronic Transactions Law 2007 Royal Decree No. M/8 8 Rabi' I- 1428H – 26 March 2007.

<sup>1875</sup> *ibid* Article 2.

also here, that due to the lack of commentary and evidential basis for cyberlaundering in Saudi Arabia, that cybercrime will be under one heading and will mainly focus on online fraud.

As regards cyberlaundering, Saudi Arabia was one of the fastest growing markets in online transactions in 2015, rising by 23% on the previous year,<sup>1876</sup> and is predicted to grow to be worth \$69 billion per annum by 2020.<sup>1877</sup> With this in mind, the growing market for online transactions is a boon for cyberlaunderers and terrorist financiers, meaning that they can flood financial institutions with small transactions to hide the origin, or destination of their money. As noted earlier, Saudi Arabian banks have specific Rules which govern their online transactions and, though Customer Due Diligence, this is meant to ensure that only identified, existing customers have access to online banking.<sup>1878</sup> However, these have been specifically criticised by MENAFATF as not covering the risks existing customers pose.<sup>1879</sup> Furthermore, the e-Transactions Law's offences are aimed at the forgery of electronic signatures and certificates,<sup>1880</sup> rather than the abuse of a legitimate system of payments to disguise transactions. Without specified offences to cover the act of cyberlaundering, as well as to address the dangers inherent within the current financial system, Saudi Arabia is at risk of cyberlaunderers using online payments to further their aims.

---

<sup>1876</sup> Payfort *Arab world could see US\$69 billion in online payment transactions per annum by 2020* (2 June 2016) <<http://www.payfort.com/press/arab-world-see-us69-billion-online-payment-transactions-per-annum-2020/>> accessed November 2016.

<sup>1877</sup> *ibid.*

<sup>1878</sup> Chapter six, 6.3.2. *supra*; Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003, Article 4.

<sup>1879</sup> *ibid* Chapter six, 6.3.2 *supra*.

<sup>1880</sup> Electronic Transactions Law 2007 Royal Decree No. M/8 8 Rabi' I- 1428H – 26 March 2007, Article 23.

With regard to online fraud, as Alanezi and Brooks outline, there is a low level of awareness of fraud in Saudi Arabia<sup>1881</sup> and, combined with the Government's "*relative silence about the activities of online fraudsters*"<sup>1882</sup> has created an impression that online fraud is not a punishable crime.<sup>1883</sup> As is further noted by Alanezi and Brooks, there is a large gap in regulation over online fraud, which means that there are no appropriate or specific laws which can guide online transactions and thus prevent fraud from occurring in Saudi Arabia.<sup>1884</sup> As El-Guindy noted as far back as 2008, "*there still need to be more specific laws for cybercrime activities*".<sup>1885</sup> As such, the Anti-Cyber Crime Law was not specifically aimed at some traditional financial crimes, such as fraud and money laundering committed through the Internet, but rather crimes against the computer, as well as crimes associated with the construction of websites to further or finance terrorism.<sup>1886</sup> It was not until 2012 that Saudi Arabia issued the Arab Cybercrime Agreement,<sup>1887</sup> which was aimed at credit card frauds, internet crimes and cyber terrorism.<sup>1888</sup> However, only this much is known about the Agreement, as well as that it looks toward increasing co-operation between Gulf States in this area of cybercrime.<sup>1889</sup> Despite the enactment of this agreement, online crime continues to rise in Saudi Arabia, now costing Saudi consumers a total of SR 21 billion a year and, per person, SR3,230.<sup>1890</sup> Consequently, it is of concern that Saudi Arabia

---

<sup>1881</sup> Alanezi, F. & Brooks, L. *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT)* Twentieth Americas Conference on Information Systems (Savannah, 2014), 7 <[aisel.aisnet.org/cgi/viewcontent.cgi?article=1156&context=amcis2014](http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1156&context=amcis2014)> accessed November 2016.

<sup>1882</sup> *ibid.*

<sup>1883</sup> *ibid.*

<sup>1884</sup> *ibid* 9.

<sup>1885</sup> El-Guindy, M. *Cybercrime in the Middle East* (ISSA Journal, 2008) <<http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf>> accessed November 2016.

<sup>1886</sup> Anti-Cyber Crime Law Article 7(2).

<sup>1887</sup> Arab Cybercrime Agreement (no. 126 of 2012).

<sup>1888</sup> Elnaïm, B.M.E. *Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future* (2013) Information and Knowledge Management Vol.3, No.12, 17.

<sup>1889</sup> *ibid.*

<sup>1890</sup> Arab News *Cybercrime hit 6.5m in Kingdom last year* (11 August 2016) <<http://www.arab-news.com/node/967966/saudi-arabia>> accessed November 2016.



has been unable to demonstrate that it has effectively investigated and prosecuted perpetrators of online fraud, given that it is susceptible to terrorist financiers.

However, as the UN Economic and Social Commission for Western Asia (ESCWA) highlighted in 2007, there is “*no evidence of legal provisions concerning data protection or processing*”.<sup>1891</sup> As noted under 6.3.2., it is difficult to assess whether Government agencies have overreached their powers of surveillance or have abused any of their existing abilities to intercept communications during the course of a criminal investigation. The lack of data protection legislation seems to be symptomatic of West Asian states, with, for example, Kuwait and Palestine also having no evidence of data protection laws<sup>1892</sup> and, as mentioned earlier, this is well within Saudi Arabia’s sovereign remit<sup>1893</sup>. Resultantly, there needs to be some form of international co-operation regarding both the level of surveillance and the degree of privacy protections afforded to Internet users while being investigated.

## **6.5. Conclusion**

Saudi Arabia has clearly made some positive movements towards legislating against terrorist financing since 2001. By becoming a founder member of MENAFATF and gaining observing membership status in the FATF, it is also clear that Saudi Arabia is willing, on the surface, to conform with international obligations regarding AML and CTF. Furthermore, through introducing transaction reporting, record-keeping, and

---

<sup>1891</sup> United Nations Economic and Social Commission for Western Asia E/ESCWA/ICTD/2007/8 *Models for Cyber legislation in ESCWA Member Countries* (27 June 2007), 16 <<https://www.unescwa.org/publications/models-cyber-legislation-escwa-member-countries>> accessed April 2018.

NB. Interestingly, since then, all of the publications relating to Cyber-legislation have been published in Arabic on the ESCWA website.

<sup>1892</sup> *ibid* 15-16.

<sup>1893</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 41.

Customer Due Diligence, as well as introducing tough new rules on donations and use of charitable funding, Saudi Arabia has heightened its potential to disrupt and deter terrorist finances from being channelled through its financial institutions and non-profit organisations. Nevertheless, with little information on how successfully its laws have been implemented, as well as scant evidence of high profile convictions using its AML and CTF legislation, it is difficult to assess how effective Saudi laws are when terrorist finances are raised both traditionally or when applied to rapidly evolving electronic technology. Additionally, the low number of Suspicious Transaction Reports for both AML and CTF, in marked contrast to the amount of projected electronic transactions being carried out in Saudi Arabia, suggests that there is under-reporting. Although the US and the UK have been previously criticised for the high level of Suspicious Activity Reports lodged with their Financial Intelligence Units, it is of concern that Saudi Arabia has so few. It therefore raises questions as to whether there is insufficient training for financial institutions or whether penalties for failing to report suspicious transactions are being rigorously applied enough, to ensure that Saudi Arabian financial institutions are no longer vulnerable to the flow of terrorist financing.

Moreover, while there is legislation in force, there is little to suggest that it is being implemented objectively and independently, with close links between the Government, financial institutions and charities remaining unmonitored. Additionally, while Saudi Arabia vigorously monitors the content of websites, having subjective criteria for blocking content without an independent regulatory body, is inappropriate by, for example the US and the UK's data protection and freedom of expression standards. While this is within the law of the Saudi authorities to undertake, mutual co-operation with countries with standards of human rights congruent with the Universal Declaration of Human Rights may be affected. Despite Snowden's revelations about

the US and the UK's monitoring of mass communications, these do not touch the extent to which Saudi authorities have control over what their citizens see and surveillance of the content of their communications. Furthermore, the Saudi definition of 'terrorism' is extremely broad under the Law of Terrorism Crimes and its Financing, including to "*undermine state reputation or status*".<sup>1894</sup> This contrasts completely with the UK, which does not include this as part of its definition of terrorism, and bases terrorism on the "*use or threat of action*"<sup>1895</sup> and the US, which uses "*violent acts*"<sup>1896</sup> or "*intimidation*"<sup>1897</sup> under the definition of international terrorism. As a result, this wide definition has also enabled Saudi authorities to use counter-terrorism laws as a way to monitor and punish those who use the Internet to voice opposition, rather than to plan or finance terrorist acts. It appears that Saudi Arabia is using a powerful weapon against what would be deemed against public morality or political disagreement, which is one of the aims of its Constitution. Finally, without comparable data protection laws in place, it is unclear how Saudi authorities monitor and intercept Internet communications and financial transactions, and, whether their methods give rise to potential abuse within the realms of their law, thus overshadowing any balance its legislation may have in appropriately finding and disrupting terrorist finances raised and channelled through the Internet. In light of this, UN and international organisations must revisit the issues of Internet governance, cybercrime and the definition of terrorism to ensure a balance is struck between effectiveness and appropriateness.

---

<sup>1894</sup> Law of Terrorism Crimes and its Financing 2013 Article 1(a).

<sup>1895</sup> Terrorism Act 2000 c.11, s. 1(1).

<sup>1896</sup> 18 U.S. Code §2331(1)(A).

<sup>1897</sup> 18 U.S. Code §2331(1)(B).

## **Chapter Seven: The United Nations and International Organisations – Conclusion**

*“One man’s terrorist is another man’s freedom fighter.”<sup>1898</sup> /  
“The problem: Finding a needle in a pile of needles”<sup>1899</sup>*

### **7.1. Introduction**

The UN response has been more gradual than that of the US and the UK towards terrorist financing. As noted in chapter three,<sup>1900</sup> prior to 9/11, the UN already had a number of resolutions designed specifically against terrorism,<sup>1901</sup> however, it was the adoption of the UN’s International Convention for the Suppression of the Financing of Terrorism in 1999 which formed the basis for the international reaction against terrorist financing after 9/11.<sup>1902</sup> Moreover, after 9/11, the UN Security Council passed Resolution 1373 on 28 September 2001, calling upon the international community to ratify the 1999 Convention and implement domestic CTF legislation, as *“such acts, like any act of international terrorism, constitute a threat to international peace and security”*.<sup>1903</sup> This had a binding effect on Member States, as it was formed under Chapter VII of the UN Charter,<sup>1904</sup> although, as noted in chapter six, it took Saudi Arabia over ten years to include the Resolution in its AML/CTF legislative framework.<sup>1905</sup> Furthermore, the UN declined to define terrorism after the 9/11 attacks,

---

<sup>1898</sup> Seymour, G. *Harry’s Game* (1st Edn. Corgi, 1975).

<sup>1899</sup> Shetterly, D., *Starving the Terrorists of Financing: How the United States Treasury is Fighting the War on Terror* (2005-2006) 18 Regent University Law Review 327, 328.

<sup>1900</sup> Chapter three, 3.2.1.1.

<sup>1901</sup> E.g. General Assembly Resolution A/RES/51/210 Measures to eliminate international terrorism (17 December 1996) calling for domestic measures on the financing of terrorism.

<sup>1902</sup> *ibid* chapter three, 3.2.1.1.

<sup>1903</sup> S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts.

<sup>1904</sup> Chapter VII United Nations Charter 1946: Action with Respect to Threats to the Peace, Breaches of the Peace and Acts of Aggression, Article 48(1).

<sup>1905</sup> Chapter six, 6.3.2.

stringently relying on the plethora of counter-terrorism Conventions to provide Member States with a guide to what could be constituted as terrorism or terrorist acts.<sup>1906</sup> Therefore, this lack of definition will be examined in light of the UN Members' different interpretations of what constitutes a terrorist act.

Moreover, 9/11 saw the rise of international organisations including the Financial Action Task Force (FATF), which issued nine Special Recommendations on the Financing of Terrorism in the wake of the attacks.<sup>1907</sup> These had been taken up by its Members and Observer countries in such numbers that by 2005, the UN Security Council had issued Resolution 1617 which “*Strongly urge[d] all Member States to implement the comprehensive, international standards embodied in the Financial Action Task Force's (FATF) Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing*”.<sup>1908</sup> Consequently, the role of the FATF must also be appraised in terms of bringing forward international standards on AML and CTF, as well as their continuing work on virtual currencies

---

<sup>1906</sup> See Annex to A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999) - UN Treaty Series 1973 *Convention for the Suppression of Unlawful Seizure of Aircraft* (16 December 1970); 974 UN Treaty Series 177 *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (23 September 1971); A/RES/3166 (XVIII) *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents* (14 December 1973); A/RES/34/146 *International Convention against the Taking of Hostages* (17 December 1979); INFCIRC/274 *Convention on the Physical Protection of Nuclear Material* (3 March 1980); 474 UN Treaty Series 1990 No. 14118 *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation* (24 February 1988); 1678 UN Treaty Series 1992 No.29004 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (10 March 1988); 1678 UN Treaty Series 1992 No.29004 *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf* (10 March 1988); A/RES/52/164 *International Convention for the Suppression of Terrorist Bombings* (15 December 1997).

<sup>1907</sup> These were issued in October 2001; FATF IX Recommendations (2001) <<http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf>> accessed November 2016.

<sup>1908</sup> S/RES/1617 (2005) Threats to international peace and security caused by terrorist acts, Article 7; Gardner, K.L. *Fighting Terrorism the FATF Way* (2007) 13(3) *Global Governance* 325, 326.

and the threats contained therein.<sup>1909</sup>

The UN is also uniquely placed to oversee the use and monitoring of the Internet, and yet it does not. This is despite growing concern over the last decade that the Internet is being used as a source of terrorist financing and the substantial Internet surveillance techniques used by some of its members, including Saudi Arabia. Instead, it issues, through the UN Human Rights Council (UNCHR), Resolutions based on the Universal Declaration of Human Rights 1948, regarding the right to privacy under Article 12<sup>1910</sup> which, unlike the Security Council's Resolutions, are non-binding. Resultantly, the issue of privacy, and how far individual Member States have taken the minimum standards under the Declaration must also be addressed.

Due to the transnational nature of both the Internet and the financing of terrorism, it is imperative that Security Council Resolution 1373, the 1999 Convention be discussed in the context of their application to Internet transactions, to find out whether the UN's approach is effective when detecting terrorist finances channelled through the Internet. Additionally, there will be an assessment of gaps in UN measures regarding the terrorist use of fast growing technology, or regulating the Internet, specifically in light of ISIL's prolific use of social media to raise finances. Moreover, an examination of the FATF's AML/CTF Recommendations is needed to assess whether its framework of detection and prevention is appropriate and effective enough to provide an international response to the financing of terrorism through the Internet.

## **7.2. Direct solicitation of donations**

---

<sup>1909</sup> E.g. Financial Action Task Force *Virtual Currencies Key Definitions and Potential AML/CTF Risks* (June 2014) <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>> accessed November 2016.

<sup>1910</sup> E.g. A/HRC/32/L.20 The promotion, protection and enjoyment of human rights on the Internet (27 June 2016).

As Internet communications are multi-jurisdictional, the UN is well-placed to oversee international measures against content of both websites and e-mails. However, traditionally, the UN has been reticent when involving itself in Internet governance<sup>1911</sup>. Consequently, Member States who are implementing their own ways of combating direct solicitations of donations currently have no international set standard to abide by. As Whitton explains, there “*are very few regulations regarding the transmission of information or what information is being transmitted*”,<sup>1912</sup> due to the lack of international co-operation,<sup>1913</sup> and the fact that the Internet is a decentralised open network.<sup>1914</sup> As such, States depend upon bilateral treaties and mutual assistance, causing concern about the quality of information exchanged, due to the fact that it must be obtained quickly before it is lost.<sup>1915</sup>

### 7.2.1. Websites

The 1999 International Convention for the Suppression of the Financing of Terrorism addresses the issue of direct solicitation of donations under Article 2, which outlines the offence of financing terrorism through “*provid[ing] or collect[ing] funds with the intention that they should be used or in the knowledge that they are to be used [for*

---

<sup>1911</sup> E.g. International involvement of only Council of Europe/Organisation for Economic and Cooperative Development. Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 11 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016.

<sup>1912</sup> Whitton, M. *Progression and Technological Advancement of Terrorist Financing: Are Current Laws Adequate?* (December 2005), 6. <[http://www.ibrarian.net/navon/paper/Progression\\_and\\_Technological\\_Advancement\\_of\\_Terr.pdf?paperid=5381481](http://www.ibrarian.net/navon/paper/Progression_and_Technological_Advancement_of_Terr.pdf?paperid=5381481)> accessed November 2016.

<sup>1913</sup> *ibid.*

<sup>1914</sup> Berman, B. *Combating Terrorist Uses of the Internet* (2005) 99 American Society of International Law Proceedings 103, 105.

<sup>1915</sup> Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 45 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016.

terrorist purposes]’.”<sup>1916</sup> Therefore, Member States are able to interpret and apply this legal framework into their own jurisdictions. The FATF goes further, stating under Recommendation 5 that countries “*should criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts*”,<sup>1917</sup> meaning that any donation to a known terrorist organisation or individual, whether they carry out an act or not, is covered, and taking away a potential defence for donors. Therefore, both the UN and FATF’s guidelines could logically be applied to a terrorist organisation which hosts a website, increasing the effectiveness of individual jurisdictions’ measures towards this type of donation.

However, as mentioned above, the issue of using potentially sympathetic states and ISPs in multiple jurisdictions to support ways of soliciting donations through websites is yet to be addressed by the UN, highlighting the need for enforceable international cooperation between jurisdictions and ISPs. Therefore, the effectiveness of finding terrorist finances raised and channelled through websites is limited to national measures, creating an advantage for terrorists, as “*regulations are very slow in coming*”.<sup>1918</sup> This can be evidenced by ISIL’s successful use of social media to propagate its aims and to entice people to join their ‘State’ in Syria and Iraq.<sup>1919</sup> As a result, the

---

<sup>1916</sup> International Convention for the Suppression of the Financing of Terrorism Adopted by the General Assembly of the United Nations in resolution A/RES/54/109 of 9 December 1999, Article 2(1).

<sup>1917</sup> Financial Action Task Force *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012, updated February 2018) <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>> accessed April 2018.

<sup>1918</sup> *ibid* Whitton, 6.

<sup>1919</sup> ISIL sent out 40,000 tweets in a single day. Irshaid, F. (BBC News, 19 June 2014) *How Isis is spreading its message online* <<http://www.bbc.co.uk/news/world-middle-east-27912569>> accessed November 2016; Neumann, P. R. *Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s* (ICSR 26 January 2015) <<http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>> accessed November 2016.; Berger, J.M. *Tailored Online Interventions: The Islamic State’s Recruitment Strategy* (Combating Terrorism Center, 23 October 2015) <<https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy>> accessed November 2016.



UN has a role to play in ensuring that Internet regulation is carried out to increase the effectiveness of individual jurisdictions' efforts to combat websites or social media sites which solicit donations.

Furthermore, by relying on private actors, such as Twitter, to monitor such communications, jurisdictions risk the possibility that right of freedom of expression and to "*seek, receive and impart information and ideas through any media...*"<sup>1920</sup> under Article 19 of the Universal Declaration of Human Rights becomes subverted. This is no more so than in the UK, where some broadband providers are now part of an 'opt in' system of Internet filtration through automatically setting parental controls and subsequently allowing users to change those filters.<sup>1921</sup> Saudi Arabia runs a website filtration system far beyond the UK, and has Government control over many of the telecommunications systems in the Kingdom, therefore the application of Article 19 becomes of even more concern, especially when private actors, such as SmartFilter, the main website filtration technology for Saudi Arabia, which is owned by McAfee, a US-based company dealing with Internet security.<sup>1922</sup> SmartFilter has also been previously used by the UK for website filtration.<sup>1923</sup> Consequently, the UN must intervene so that website filtration is used appropriately.

Moreover, without a proper definition of terrorism, countries' use of counter-terrorism and surveillance powers vary widely, with little specific guidance from UN Conventions or Resolutions to distinguish between websites which solicit donations

---

<sup>1920</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A), Article 19.

<sup>1921</sup> Chapter five, 5.2.1.

<sup>1922</sup> York, J.C. (Al Jazeera, 29 March 2011) *The booming business of Internet censorship* <<http://www.aljazeera.com/indepth/opinion/2011/03/2011329113450125509.html>> accessed November 2016.

<sup>1923</sup> Glanville, J. (The Guardian, 17 November 2008) *The big business of net censorship* <<https://www.theguardian.com/commentisfree/2008/nov/17/censorship-internet>> accessed November 2016.

for a terrorist cause and those which offer an alternative political or religious viewpoint. The language of the 1999 Convention is vague, failing to define “terrorism”,<sup>1924</sup> and relying on other Conventions to provide a general guideline to what it means.<sup>1925</sup> The UN General Assembly in 1999 also condemned “*criminal acts intended or calculated to provoke a state of terror in the general public... for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them*”,<sup>1926</sup> but still shied away from a full definition of terrorism.

The 1999 Convention also states quite clearly that signatories are “*to ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature*”.<sup>1927</sup> Yet, as mentioned chapter six, Saudi Arabia is still able to imprison Raif Badawi and others under its counter-terrorism laws for setting up humanitarian and political websites, which run contrary to the country’s moral principles.<sup>1928</sup> The UN Security Council has some Resolutions which seek to narrow the field of terrorist organisations, most notably through Resolution 1267 which imposes freezing sanctions and travel bans on the Taliban and Osama bin Laden,<sup>1929</sup> extending this to al-Qaeda in Resolution 1333,<sup>1930</sup> binding Member States to apply freez-

---

<sup>1924</sup> Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 27, 33 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016 – discussion of “information terrorism”.

<sup>1925</sup> Ibid.

<sup>1926</sup> UN General Assembly Resolution A/RES/53/108 Measures to eliminate international terrorism (26 January 1999).

<sup>1927</sup> A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999), Article 6.

<sup>1928</sup> See chapter six, 6.2.1.

<sup>1929</sup> S/RES/1267 (1999) on Afghanistan.

<sup>1930</sup> S/RES/1333 (2000) on the situation in Afghanistan.

ing sanctions to those on the ISIL and al-Qaeda Designated Sanctions List under Resolution 2253<sup>1931</sup> and ‘unequivocally condemning’ ISIL under Resolution 2249.<sup>1932</sup> However, the UN does not hold a list of proscribed organisations,<sup>1933</sup> leaving it to Member States to decide which organisations or individuals they deem to be of terrorist threat. Without a clear definition of what terrorism is at an international level, it remains that some countries will go as far as they need to in order to, potentially, quell dissent under the guise of counter-terrorism. As Walter notes, “[t]errorism is... a convenient term for circumscribing certain activities which ‘are widely disapproved of’”.<sup>1934</sup> It is not within the remit of this thesis to define terrorism per se or to argue the types of definition, but it is necessary to mention that the 1999 Convention goes some way to refer to terrorism as a violent act<sup>1935</sup> or an act of intimidation.<sup>1936</sup> This is broadly concurrent with the UK and US definitions,<sup>1937</sup> which centre around the act and threat of action. Consequently, should the UN decide to define terrorism, it may be worthwhile if it is based around a narrower scope such as this, in order to prevent jurisdictions from over-using their counter-terrorism laws, especially when dealing with freedom of expression through websites.

### 7.2.2. Electronic Communications

---

<sup>1931</sup> S/RES/2253 (2015) Threats to international peace and security caused by terrorist acts.

<sup>1932</sup> S/RES/2249 (2015) Threats to international peace and security caused by terrorist acts.

<sup>1933</sup> The Sanctions Lists are only applicable to those individuals and organisations connected with al-Qaeda, the Taliban and ISIL, not other terrorist groups. See UN Security Council <<https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>> accessed November 2016.

<sup>1934</sup> Walter, C. *Defining Terrorism in National and International Law* (2004), 22. <[https://www.unodc.org/tldb/bibliography/Biblio\\_Terr\\_Def\\_Walter\\_2003.pdf](https://www.unodc.org/tldb/bibliography/Biblio_Terr_Def_Walter_2003.pdf)> accessed November 2016.

<sup>1935</sup> A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999), Article 2(1)(b).

<sup>1936</sup> *ibid*; *ibid* Walter, C. *Defining Terrorism in National and International Law* (2004), 12.

<sup>1937</sup> Chapter three, US definition under 18 U.S. Code §2331(1).

In response to concerns that the UN was not adequately addressing changing technologies used in terrorist financing, its Counter-Terrorism Strategy was formulated in 2006, setting out the need for UN involvement in counteracting the use of the Internet by terrorists.<sup>1938</sup> Under the Strategy, the UN is to “*explore ways and means to coordinate efforts at the international and regional level to counter terrorism in all its forms and manifestations on the Internet*”<sup>1939</sup> and “*use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard.*”<sup>1940</sup> Moreover, the UN set up a Working Group to identify ways and means of counteracting terrorist financing through the Internet.<sup>1941</sup> The Working Group’s actions included identifying three strategies for UN Member States to adopt: (a) General cybercrime legislation; (b) General (non-Internet-specific) counter-terrorism legislation and (c) Internet-specific counter-terrorism legislation.<sup>1942</sup> This represents some step towards finding an effective global solution towards preventing the financing of terrorist acts through the Internet.

As regards appropriateness, Article 8(1) of the 1999 Convention broadly states that each Party State shall “*take appropriate measures, in accordance with its domestic legal principles*”<sup>1943</sup> to detect terrorist financing. However, this fails to define

---

<sup>1938</sup> A/RES/60/288 United Nations *Global Counter-Terrorism Strategy* (8 September 2006) Annex Title II, 12 <<https://www.un.org/counterterrorism/ctitf/en/un-global-counter-terrorism-strategy>> accessed November 2016.

<sup>1939</sup> Title II Paragraph 12(a) *Global Counter-Terrorism Strategy*.

<sup>1940</sup> *ibid* 12(b).

<sup>1941</sup> The Working Group on Countering the use of the Internet for Terrorist Purposes held a series of conferences to evaluate the use of the Internet for terrorist purposes, United Nations Office on Drugs and Crime *Use of the Internet for terrorist purposes* (September 2012), 1 <[http://www.unodc.org/documents/frontpage/Use of Internet for Terrorist Purposes.pdf](http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf)> accessed November 2016.

<sup>1942</sup> United Nations Counter-Terrorism Implementation Task Force Working Group Compendium *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects* (May 2011), 6-7. <[http://www.un.org/en/terrorism/ctitf/pdfs/ctitf\\_interagency\\_wg\\_compendium\\_legal\\_technical\\_aspects\\_web.pdf](http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf)> accessed November 2016.

<sup>1943</sup> A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999), Article 8(1).

which measures would be explicitly intrusive. Consequently, this makes the closure of websites and the surveillance of private communications subjective to particular domestic laws, rather than an objectively defined standard, generating criticism as to its appropriateness.<sup>1944</sup> Moreover, as Aldrich highlights, although the Universal Declaration of Human Rights provides a freedom to seek and impart information through media communications,<sup>1945</sup> it has a number of broad exceptions which allow law enforcement agencies to intercept communications.<sup>1946</sup> For example, under Article 29(1) of the Declaration, “*everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society*”,<sup>1947</sup> meaning that national security requirements are exempted. As a result, this wide application and allowance for states to decide their own levels of surveillance is concerning for privacy rights. For instance, as Drozdova outlined as early as 2000, the use of intrusive surveillance on internet users could inevitably be abused by governments under their own domestic laws for the aim of suppression.<sup>1948</sup> This has clearly been evidenced by the use of counter-terrorism laws by Saudi Arabia to suppress anti-government rhetoric,<sup>1949</sup> as well as used by the UK and the US as a basis for their mass surveillance

---

<sup>1944</sup> Drozdova, E.A. CISAC Report: *Civil liberties and security in cyberspace* (2000) <[https://cisac.fsi.stanford.edu/publications/civil\\_liberties\\_and\\_security\\_in\\_cyberspace](https://cisac.fsi.stanford.edu/publications/civil_liberties_and_security_in_cyberspace)> accessed June 2018.

<sup>1945</sup> Under Article 19 Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A); Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies, 53 <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016.

<sup>1946</sup> *ibid* Aldrich.

<sup>1947</sup> Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A), Article 29(1).

<sup>1948</sup> *ibid* Drozdova, E.A. *CISAC Report: Civil liberties and security in cyberspace* (2000), 13-14.

<sup>1949</sup> Chapter six, 6.2.2.

techniques revealed by Edward Snowden.<sup>1950</sup> Consequently, it is clear that an international standard is needed through some governance of the Internet, in order to increase the effectiveness of finding terrorist finances while equally limiting the potential abuses of intrusive surveillance.

Here, the UN Human Rights Council (UNHRC) has been more proactive in outlining freedom of expression and privacy rights for Internet users. For example, the UNHRC has introduced a number of Resolutions since 2009 which confer privacy and freedom of expression principles to the use of the Internet. For example, in 2009, the Council called on all states to “*refrain from using counter-terrorism as a pretext to restrict the right to freedom of opinion and expression in ways that are contrary to their obligations under international law*”<sup>1951</sup> and recognised “*the positive contribution that the exercise of the right to freedom of expression, particularly by the media, including through information and communication technologies such as the Internet*”.<sup>1952</sup> The Council further extended the point of freedom of expression to Internet communications in 2012, affirming that “*the same rights that people have offline must also be protected online, in particular freedom of expression*”,<sup>1953</sup> reaffirmed in 2014<sup>1954</sup> and 2016, with the 2016 Resolution particularly condemning “*measures to intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law*”,<sup>1955</sup> potentially capturing large scale sur-

---

<sup>1950</sup> Chapter four, 4.2.2. and chapter five, 5.2.2.

<sup>1951</sup> A/HRC/RES/12/16 on the Promotion and Protection of all human rights, civil political, economic, social and cultural rights, including the right to development (2 October 2009), Article 5(1)(o).

<sup>1952</sup> *ibid* Article 9.

<sup>1953</sup> A/HRC/20/L.13 The promotion, protection and enjoyment of human rights on the Internet (29 June 2012), Article 1.

<sup>1954</sup> A/HRC/26/L.24 The promotion, protection and enjoyment of human rights on the Internet (26 June 2014).

<sup>1955</sup> A/HRC/32/L.20 The promotion, protection and enjoyment of human rights on the Internet (27 June 2016), Article 10.

veillance and filtration operations carried out by the UK, US and Saudi Arabia. Additionally, UNHRC Resolution 28/16<sup>1956</sup> appoints a Special Rapporteur<sup>1957</sup> to assess whether countries have breached online privacy, again addressing some of the concerns surrounding mass data collection and the steady erosion of privacy since more stringent counter-terrorism laws had been introduced following 9/11. However, these Resolutions do not have the same effect as Security Council Resolutions, by their very nature, they are non-binding,<sup>1958</sup> thus they do not ensure that Member States adhere to the principles of privacy and freedom of expression when intercepting communications.

Despite the concerns about the non-binding nature of these Resolutions, the UN General Assembly has also issued several Resolutions which aim to combat the potential abuse of powers which monitor email and social media communications. In 2014, General Assembly Resolution 68/167 regarding online privacy was passed, which called upon Member States to review the practices, procedures and legislation on surveilling communications, interception and the collection of personal data, which includes mass surveillance,<sup>1959</sup> and reaffirming that “*States must ensure that any measures taken to combat terrorism are in compliance with their obligations under international law*”.<sup>1960</sup> This has been further amplified by General Assembly Resolution 69/166 in 2015.<sup>1961</sup> While technically, these could prevent members from carrying out large scale surveillance techniques and, on the surface, has been observed by

---

<sup>1956</sup> A/HRC/RES/28/16 The right to privacy in the digital age (1 April 2015).

<sup>1957</sup> *ibid* Article 4.

<sup>1958</sup> The UNHRC is not a principal organ of the UN, such as the General Assembly, the UN Security Council, the Economic and Social Council as well as the International Court of Justice under Article 7(1) of the UN Charter. Simma, B, Khan, D.E., Nolte, G. Paulus, A. (ed.) *The Charter of the United Nations: A Commentary* (3<sup>rd</sup> Ed. Oxford University Press, 2012), 1943.

<sup>1959</sup> A/RES/68/167 The right to privacy in the digital age (21 January 2014), Article 4(c).

<sup>1960</sup> *ibid* [11].

<sup>1961</sup> A/RES/69/166 The right to privacy in the digital age (10 February 2015).

the US,<sup>1962</sup> the UK is still planning to continue bulk surveillance measures under the Investigatory Powers Act,<sup>1963</sup> taking steps to gather further data information through Internet Connection Records.<sup>1964</sup> Therefore, such measures by the UN General Assembly through non-binding Resolutions<sup>1965</sup> are not effective enough to ensure that its members are using their powers appropriately within the confines of international law.

To that end, the issue of Internet governance by the UN should be revisited, in order to effectively and appropriately monitor Internet communications. Johnson and Post argue that, due to the fact communications can be spread beyond the physical jurisdiction of a server, cyberspace "*undermines the relationship between legally significant phenomena and physical location*".<sup>1966</sup> As Hamilton further notes, "*rules regarding which jurisdiction's laws might be applicable in a particular dispute may vary from country to country*".<sup>1967</sup> This is no more evident than in the case of Yahoo!, eventually heard before the US Court of Appeals.<sup>1968</sup> Yahoo!, an internet search engine, unsuccessfully argued that it should continue to allow Nazi paraphernalia to be listed on its auction service, in breach of French anti-Semitism laws.<sup>1969</sup> In this case, the Court surmised that the District Court of California had no jurisdiction over France, therefore France was able to apply its laws to Yahoo!.<sup>1970</sup> This case clearly

---

<sup>1962</sup> Under the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 ("USA Freedom Act") (Pub. L. 114-23, 120 Stat 200) (50 U.S.C. 1801). See chapter four at 4.2.2. and chapter five at 5.2.3.a. for further information.

<sup>1963</sup> Chapter five at 5.2.3.a. and 5.2.3.b.

<sup>1964</sup> *ibid* chapter five at 5.2.3.

<sup>1965</sup> NB. Again, the General Assembly does not have the same powers as the UN Security Council in having binding Resolutions.

<sup>1966</sup> Johnson, D.R. & Post, D.G. *Law and Borders: The Rise of Law in Cyberspace*, (1996) 48 Stanford Law Review 1367, 1370.

<sup>1967</sup> Hamilton, L. *Regulation of the Internet: An impossible task?* (2010) 4 Galway Student L. Rev. 33, 35.

<sup>1968</sup> *Yahoo! Inc. v. La Ligue le Racisme et L'Antisemitisme* 145 F. Supp. 2d 1168 (N.D. Cal. 2001).

<sup>1969</sup> *ibid*; Hamilton, L. *Regulation of the Internet: An impossible task?* (2010) 4 Galway Student L. Rev. 33, 35; Reidenberg, J.R. *Technology and Internet Jurisdiction* (2005) 153 U. Pa. L. Rev. 1951, 1952.

<sup>1970</sup> *ibid* Reidenberg. J.R..



shows the jurisdictional difficulties in applying certain Internet laws, which also applies in terrorist use of the Internet to communicate and solicit donations. These difficulties are amplified by the use of ISPs, essentially private actors, to enforce each jurisdiction's counter-terrorism legislation and cyberlaws. Consequently, the UN is significantly well-placed to ensure that independent oversight covers Internet communications, rather than leave it to individual jurisdictions, which must contend with competing interests in other jurisdictions, or with laws which subvert the Universal Declaration of Human Rights.

This issue was first visited by the UN's World Summit on the Information Society (WSIS) in 2003, which identified under Principle 5 that "[i]t is necessary to prevent the use of information... technologies for criminal and terrorist purposes while respecting human rights...".<sup>1971</sup> Furthermore, the WSIS proposed four models of Internet governance, ranging from no international organisational oversight, to a Global Internet Council.<sup>1972</sup> Consequently, it is clear that the UN was working towards an effective, international way of governing Internet use, while attempting to balance this with the privacy of many Internet users.

The International Telecommunications Union, a subsidiary of the UN,<sup>1973</sup> went

---

<sup>1971</sup> United Nations World Summit on the Information Society *Geneva Declaration of Principles* (2003) Document WSIS-03/GENEVA/DOC/4-E, Principle 5(5) <[http://www.itu.int/dms\\_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf)> accessed November 2016; also see United Nations World Summit on the Information Society *Second Phase – Tunis Commitments* (2005) [15] Document WSIS-05/TUNIS/DOC/7-E <<http://www.itu.int/wsis/docs2/tunis/off/7.pdf>> accessed November 2016.

<sup>1972</sup> United Nations *Report of the Working Group on Internet Governance* (2005), 12-16 <[www.wgig.org/docs/WGIGREPORT.pdf](http://www.wgig.org/docs/WGIGREPORT.pdf)> accessed November 2016.

<sup>1973</sup> This became a specialised agency of the UN in 1947 – Agreement between the United Nations and the International Telecommunications Union (1949).

further, proposing a Treaty in 2012 at the World Conference on International Telecommunications (WCIT-12),<sup>1974</sup> which has stepped into the realms of Internet governance, including measures on suspension of Internet services.<sup>1975</sup> However, the Regulations were severely criticised by some Permanent UN Security Council (UNSC) members, such as the US, which unanimously voted in Congress on a resolution to oppose UN governance of the Internet,<sup>1976</sup> stating that it would continue to “*promote a global Internet free from government control and preserve and advance the successful multistakeholder model that governs the Internet today*”,<sup>1977</sup> as evidenced by the US Government’s release of Internet Corporation for Assigned Names and Numbers (ICANN)<sup>1978</sup> stewardship away from Government control and into the hands of Internet multi-stakeholders<sup>1979</sup> in 2016.<sup>1980</sup> Furthermore, the European Parliament also passed a resolution on the WICT-12 just before the conference,<sup>1981</sup> stating

---

<sup>1974</sup> This was attended by representatives of 193 countries – International Telecommunications Union *World Conference on International Telecommunications (WCIT-12)* (3-14 December 2012) <<http://www.itu.int/en/wcit-12/Pages/default.aspx>> accessed November 2016.

<sup>1975</sup> International Telecommunications Union *International Telecommunication Regulations* (14 December 2012), Article 7 <<https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf>> accessed November 2016.

<sup>1976</sup> US House of Representatives *Expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived* 112th Congress, H.Con.Res.127 (2 August 2012) <<https://www.congress.gov/bills/112th-congress/house-concurrent-resolution/127/text>> accessed November 2016.

<sup>1977</sup> *ibid.*

<sup>1978</sup> Formed in 1998 as a private entity to register domain names across the Internet, ICANN was subject to a Memorandum of Understanding with the United States Department of Commerce, Kruger, L. R42351 *CRS report to Congress Internet Governance and the Domain Name System: Issues for Congress* (18 November 2016), 2 <<https://fas.org/sgp/crs/misc/R42351.pdf>> accessed June 2018.

<sup>1979</sup> This is a bottom-up approach to Internet governance which is modelled by ICANN and has some input into Government policy – see Malcolm, J. *Multi-Stakeholder Governance and the Internet Governance Forum* (1<sup>st</sup> Edn. Terminus Press, 2008), 40.

<sup>1980</sup> *ibid* 4-5.

<sup>1981</sup> European Parliament *European Parliament resolution of 22 November 2012 on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations* (2012/2881(RSP), European Parliament, 2012) <<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0451&language=EN&ring=P7-RC-2012-0498>> accessed November 2016.

that “*the ITU, or any other single, centralised international institution, is not the appropriate body to assert regulatory authority over either internet governance or internet traffic flows*”.<sup>1982</sup> Consequently, despite some amendments to the Regulations, the US, the UK and France all declined to sign them, whereas Russia, China and Saudi Arabia were signatories.<sup>1983</sup>

This divide between divesting political control of the Internet and the requirement of international Internet governance was also clear when UN Member States and Permanent Members of the UNSC, Russia and China, along with Tajikistan and Uzbekistan, attempted to introduce a Code of Conduct in 2011.<sup>1984</sup> Under these proposals, Member States would voluntarily sign up to a code which included co-operating in preventing online terrorist and criminal activities, incorporating “*curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries’ political, economic and social stability, as well as their spiritual and cultural environment*”.<sup>1985</sup> Unsurprisingly, the incorporation of “*spiritual and cultural environment*” within the dissemination of information steps beyond the realms of, for example, the US and UK definitions of terrorism and could have had a negative impact on freedom of expression principles under the Universal Declaration. Furthermore, this form of government control was unacceptable to, for example, the US, which is a strong proponent of the multi-stakeholder approach to Internet governance. It therefore appears that, while the UN is working towards a model of Internet governance, which may eventually equalise the way in which countries use their

---

<sup>1982</sup> *ibid* s.(C)3.

<sup>1983</sup> International Telecommunications Union *Signatories of the Final Acts* <<http://www.itu.int/osg/wcit-12/highlights/signatories.html>> accessed November 2016.

<sup>1984</sup> NATO A/66/359 *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (NATO Cooperative Cyber Defence Centre of Excellence, 14 September 2011) <[https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct\\_0.pdf](https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf)> accessed November 2016.

<sup>1985</sup> *ibid* (c).

surveillance techniques, without compromise and agreement from all Member States, such a Treaty or Convention is still a long way off, leaving terrorist organisations such as ISIL to evolve communications using the latest technology.

### **7.3. Using legitimate sources**

After 9/11, the UN and international organisations both led the charge against terrorist financing through UN Security Council Resolution 1373, which bound Member States to apply the 1999 Convention. As part of this, the FATF implemented its recommendations, which provided guidance and clarity to the UN's Convention, as well as peer-to-peer monitoring processes thorough Mutual Evaluation Reports. As such, the evolution of terrorist financing through donating online to charities and using online services of financial institutions refers back to both the 1999 Convention and the FATF Recommendations.

#### **7.3.1. Charities**

Both the UN and FATF have been prolific in providing measures which prevent terrorists using non-profit organisations as a front.<sup>1986</sup> For example, the FATF, implementing Resolution 1373 under Recommendation 6, sets out the framework for targeting individuals and organisations which provide support to terrorist activities through financial sanctions.<sup>1987</sup> For instance, under Recommendation 8, member countries “*should review the adequacy of laws and regulations that relate to entities*

---

<sup>1986</sup> Bantekas, I. *The International Law of Terrorist Financing* (2003) 97 American Journal of International Law 315, 321-2.

<sup>1987</sup> Financial Action Task Force *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (2012, updated February 2018) Recommendation 6, [13] <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>> accessed April 2018.

that can be abused for the financing of terrorism...”,<sup>1988</sup> providing “Best Practice” guidance, including financial transparency,<sup>1989</sup> verification of activities<sup>1990</sup> and due diligence.<sup>1991</sup> The Recommendation also notes that there are ways in which terrorist organisations use charities including: (a) posing as legitimate entities; (b) exploiting legitimate entities as conduits for terrorist financing; and (c) concealing or obscuring the clandestine diversion of funds intended for legitimate purposes to terrorist organisations.<sup>1992</sup> Consequently, there is a clear international framework in relation to preventing finances from being channelled through non-profit organisations.

Moreover, the UN focuses upon donors, using the 1999 Convention and Resolution 1373 to require countries to freeze assets of both individuals and organisations,<sup>1993</sup> enabling law enforcement agencies to investigate potential terrorist financing links, while providing a preventative measure by cutting off the source of funds through asset freezing. However, the effectiveness of Recommendation 6 on targeted sanctions by the FATF has been criticised by Thony and Png, on the basis that the majority of countries struggle to comply fully with its measures.<sup>1994</sup> This is exemplified by Saudi Arabia, which did not even have specific CTF legislation or specific application of Resolution 1373 until 2014.<sup>1995</sup> Moreover, these measures rely on

---

<sup>1988</sup> *ibid.*

<sup>1989</sup> Financial Action Task Force *Combating the Abuse of Non-Profit Organisations - International Best Practices* (June 2015), [61], 26 <<http://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf>> accessed November 2016.

<sup>1990</sup> *ibid* [59].

<sup>1991</sup> *ibid* [49, 50], 22.

<sup>1992</sup> Recommendation 8, FATF.

<sup>1993</sup> 1999 International Convention on the Suppression of Terrorism, Article 8(1).

<sup>1994</sup> Thony, J.F. & Png Cheong, A. *FATF Special Recommendations and UN Resolutions on the Financing of Terrorism: A review of the status of implementation and legal challenges faced by countries* (2007) 14(2) *Journal of Financial Crime* 150, 154; Baldwin, F.N. *The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?* (2004) 8(2) *Journal of Money Laundering Control* 127, 128.

NB. They refer to the Special Recommendation III which was later replaced by Recommendation 6 in 2012.

<sup>1995</sup> See chapter six, 6.2.1. for further information.

finding the identity of the donor, again a difficulty when the Internet can be used as an anonymous medium.<sup>1996</sup> Consequently, both Resolution 1373 and Special Recommendation III are difficult to enforce internationally, limiting their effectiveness further.

Additionally, the appropriateness of asset freezing can vary from country to country, even those with extensive experience of CTF. For instance, the UK's regime of asset freezing was criticised in the UK case of *HM Treasury v Ahmed and others*,<sup>1997</sup> whereby the UK Supreme Court, as outlined in chapter five,<sup>1998</sup> found that the UK Government had acted ultra vires by taking its freezing orders outside the scrutiny of Parliament.<sup>1999</sup> Furthermore, the US case of *KindHearts for Charitable Humanitarian Development Inc v Timothy Geithner et al.*<sup>2000</sup> showed that the District Court of Ohio had been 'arbitrary' when applying freezing orders.<sup>2001</sup> Therefore, this creates concern as to whether the most important aspect of the UN's reaction to terrorist financing is truly appropriate, and whether it balances the need for preventative and investigative measures properly against human rights.

### **7.3.2. Financial Institutions**

Primarily, the UN uses the implementation of the 1999 Convention to set international levels on preventing the use of financial institutions by terrorists through the Internet. For instance, under Article 18 of the UN Convention, financial institutions are required

---

<sup>1996</sup> Bantekas, 324.

<sup>1997</sup> *HM Treasury v Mohammed Jabar Ahmed and others; Her Majesty's Treasury v Mohammed al-Ghabra; R (on the application of Hani El Sayed Sabaei Youssef) v Her Majesty's Treasury* [2010] UKSC 2.

<sup>1998</sup> See chapter five, 5.3.1. for further information.

<sup>1999</sup> *ibid.*

<sup>2000</sup> *KindHearts for Charitable Humanitarian Development Inc v. Timothy Geithner et al.* Case 3:08cv 02400 (18 August 2009).

<sup>2001</sup> *ibid* chapter five 5.3.1.

to file suspicious activity reports<sup>2002</sup> and to promote customer identification.<sup>2003</sup> Moreover, the Financial Action Task Force again relies upon Resolution 1373 in order to carry out its role in preventing terrorist funding through financial institutions,<sup>2004</sup> focusing on reporting requirements by using Recommendation 20. Overall, this places the burden again on private institutions such as banks to monitor accounts and global financial flows. Yet, as can be seen with the US and the UK, because of severe penalties due to AML/CTF provisions,<sup>2005</sup> there is a huge amount of over-reporting in this area. As noted previously,<sup>2006</sup> there were fraud alerts on the bank accounts of some of the 9/11 terrorists, but these had been missed by US law enforcement authorities.<sup>2007</sup> Coupled with the sheer amount of online transactions, this focus on reporting therefore creates a system whereby banks and financial institutions report so many suspicious activities generate so much data that it is like looking for a needle in a pile of needles. As outlined in chapter five, this task is made more difficult when financial institutions, such as HSBC, have knowingly covered up instances of money laundering and terrorist financing.<sup>2008</sup> Furthermore, the international picture on the effectiveness of reporting is bleak; while financial institutions in the US and UK over-report suspicious transactions, countries such as Saudi Arabia significantly under-report.<sup>2009</sup> This lack of genesis between financial institutions and their reporting procedures mean that the effectiveness of both the FATF and the UN are hampered.

---

<sup>2002</sup> Article 18(1)(b)(iii).

<sup>2003</sup> 1999 Convention on the Suppression of Terrorism, Article 18(1)(b)(i) and (ii); Bantekas at p325

<sup>2004</sup> Morais, H. V. *Fighting International Crime and its financing: The importance of following a coherent global strategy based on the rule of law* (2005) 50 Villanova Law Review 583.

<sup>2005</sup> See chapter four 4.3.2. and chapter five 5.3.2. for further information.

<sup>2006</sup> *ibid* chapter four, 4.3.2.

<sup>2007</sup> *ibid*.

<sup>2008</sup> Chapter five, 5.3.2.

<sup>2009</sup> Chapter six, 6.3.2.

Furthermore, although the UN's measures are the most far reaching, spanning over 192 Member States, and have the potential to unify global attitudes towards terrorism, its reaction towards raising online funds through financial institutions has been criticised on several bases. Essentially, there is no international co-ordinated effort in terms of locating systems of terrorist wealth transfer<sup>2010</sup> or in specifically legislating against terrorist use of online banking. Moreover, the effectiveness of focusing on overall reporting requirements for banks has been criticised by Passas, who states with reference to 9/11, that "*none of the [Special Recommendations] would have red flagged any of the hijackers' transactions if they had been in place before the attacks...*".<sup>2011</sup> Without the necessary capabilities of finding terrorist transactions online, the effectiveness of such measures is further compromised. Therefore, the UN and the FATF again fail to address the problems of, or provide assistance regarding reporting requirements, so that financial institutions may be able to target specific transactions, rather than dealing with an increasing flow of information.

However, in 2013, the FATF issued guidance on New Payment Products and Services,<sup>2012</sup> which identified the risk of using pre-payment cards, and online transactions. The Guidance relies on financial institutions using Customer Due Diligence, as well as using limits to make the amount of transactions low,<sup>2013</sup> thereby mitigating the risk of money laundering and terrorist financing. Yet, these do not combat the risk of 'cheap terrorism', which has risen substantially since 9/11,<sup>2014</sup> including attacks on

---

<sup>2010</sup> Levitt, M. *Stemming the flow of terrorist financing: practical and conceptual challenges* (2003) 27(1) Fletcher Forum of World Affairs 63, 64.

<sup>2011</sup> Passas, N. *Informal Value Transfer Systems and Criminal Organisations: A Study into so-called Underground Banking Networks* (1999), 3.

<sup>2012</sup> *FATF Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services* (June 2013) <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>> accessed November 2016.

<sup>2013</sup> *ibid* 14-15.

<sup>2014</sup> Chapter five, 5.2.2.



London, Madrid, Lee Rigby and the Boston Bombings, all of which were carried out at a low cost.<sup>2015</sup> Unlike money laundering, whereby it is relatively easy for financial institutions to implement specific computer algorithms to find out patterns of transactions during the layering process,<sup>2016</sup> there is no such equivalent for terrorist financing.<sup>2017</sup> The FATF noted in 2008 that “[w]hile low value transactions do not necessarily equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky...”,<sup>2018</sup> virtually writing off the impact cheap terrorism can have. This fundamental gap in international guidance is of fundamental concern, as this provides terrorist with a key ability to avoid detection, should they carry out small transactions in countries with weak AML/CTF provisions. As a result, the FATF recommendations are rendered virtually redundant in cases of terrorist financing which fall below the traditional suspicious activity reporting limits. It is therefore imperative that both national governments and international organisations such as the UN are more proactive when dealing with the causes of terrorism, alongside the monitoring of transactions.

Nevertheless, in 2014, the FATF undertook a wide-ranging study into virtual currencies, and the AML/CTF risks inherent in their use.<sup>2019</sup> Particularly, the use of virtual wallet currencies, such as Bitcoin, which can be converted into cash, were identified by the FATF as high risk as they allow greater anonymity due to the fact that

---

<sup>2015</sup> *ibid.*

<sup>2016</sup> Roth, J., Greenberg, D. Wille, S. *National Commission on Terrorist Attacks Upon the United States Staff Monograph on Terrorist Financing* (2004) <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018.

<sup>2017</sup> *ibid.*

<sup>2018</sup> Financial Action Task Force *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (18 June 2008) [4], 2 <<http://www.fatf-gafi.org/documents/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercial-websitesandinternetpaymentsystems.html>> accessed November 2016.

<sup>2019</sup> Financial Action Task Force *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014) <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>> accessed November 2016.

they can be traded on the Internet,<sup>2020</sup> are generally characterised by non-face-to-face customer relationships,<sup>2021</sup> and “*may also permit anonymous transfers, if sender and recipient are not adequately identified*”.<sup>2022</sup> Furthermore, the FATF identified that virtual currencies can be used to make cross-border payments and transfers.<sup>2023</sup> The problem of identification, as the FATF further surmised, is made more difficult because of complex infrastructures used by these currencies, which involve several entities to transfer funds.<sup>2024</sup> By using several entities across a number of countries, customer identification records will be held in different jurisdictions,<sup>2025</sup> which may have inadequate AML/CTF provisions.<sup>2026</sup> This makes the traditional forms of record-keeping, reporting and customer identification procedures even more difficult for law enforcement authorities to trace. As the FATF further notes, the problem is further intensified due to the different types of virtual currency systems available, as “[c]entralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes”.<sup>2027</sup> If virtual currencies are decentralised, or not governed by one specific entity, they could also allow anonymous transactions which “*exist in a digital universe entirely outside the reach of any particular country*”.<sup>2028</sup> Consequently, law enforcement authorities based in different jurisdictions are faced with a mammoth task in tracking and tracing terrorist finances raised and channelled through virtual currencies. Although there have been some successes in the US with Silk Road and Liberty Reserve, which were found to

---

<sup>2020</sup> *ibid* 9.

<sup>2021</sup> *ibid.*

<sup>2022</sup> *ibid.*

<sup>2023</sup> *ibid.*

<sup>2024</sup> *ibid* 10.

<sup>2025</sup> *ibid.*

<sup>2026</sup> *ibid.*

<sup>2027</sup> *ibid.*

<sup>2028</sup> *ibid.*

have helped finance criminal activities online,<sup>2029</sup> with countries such as Saudi Arabia, whose AML/CTF has only recently conformed with international standards,<sup>2030</sup> it is difficult to see how this type of financing can be stemmed through financial institutions.

#### 7.4. Cybercrime

The UN has been aware of the criminal misuse of information technologies since the 1990s.<sup>2031</sup> For example, Resolutions 55/63<sup>2032</sup> and 56/121<sup>2033</sup> have incorporated concerns about the use of information technologies by terrorists and criminals.<sup>2034</sup> As Akindemowo outlines, the broad definitions provided by the 1999 Convention can include newer, more informal ways of transferring funds for terrorist purposes,<sup>2035</sup> for instance, virtual currencies. After 9/11, the UN and the FATF again focused on customer due diligence procedures by financial institutions<sup>2036</sup> and reporting requirements,<sup>2037</sup> concentrating on traditional tools of detection<sup>2038</sup> while at the same time

---

<sup>2029</sup> See Chapter four 4.2.2. for further information; *US Grand Jury Sealed Indictment United States v. Liberty Reserve S.A. Arthur Budovsky, Vladimir Katz, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jimenez, Azzeddine El Amine, Mark Marmilev and Maxim Chukharev* (2013) S.D.N.Y. 13 Crim 368.

<sup>2030</sup> Chapter six, 6.2.

<sup>2031</sup> E.g. Resolution A/RES/45/121 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (14 December 1990).

<sup>2032</sup> Resolution A/RES/55/63 Combating the criminal misuse of information technologies (4 December 2000).

<sup>2033</sup> Resolution A/RES/56/121 Combating the criminal misuse of information technologies (19 December 2001); Akindemowo, O.E. *The pervasive influence of anti-terrorist financing policy: post 9/11 non bank electronic money issuance* (2004) 19(8) Journal of International Banking Law and Regulation 289, 291 (fn40).

<sup>2034</sup> *ibid.*

<sup>2035</sup> *ibid.*

<sup>2036</sup> Akindemowo, O.E. *The pervasive influence of anti-terrorist financing policy: post 9/11 non bank electronic money issuance* (2004) 19(8) Journal of International Banking Law and Regulation 289, 296; Financial Action Task Force *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (18 June 2008), [133], 36 <<http://www.fatf-gafi.org/documents/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsiteandinternetpaymentsystems.html>> accessed November 2016.

<sup>2037</sup> *ibid.*

<sup>2038</sup> Whitton, 17.

outlining concern about adverse outside effects upon the growth of the e-money market.<sup>2039</sup> Moreover, as outlined above, the UN is still silent about formulating an International Treaty on either regulating the Internet<sup>2040</sup> or cybercrime.<sup>2041</sup> Again, this causes problems with effectiveness, due to limited jurisdictional aspects of individual Member States and failing to address the fact that cybercrime is a global phenomenon.<sup>2042</sup> During the first years of the 21<sup>st</sup> Century, the UN concentrated on increasing access to the Internet through the World Summit on the Information Society (WSIS), which outlined a number of Principles.<sup>2043</sup> Under Principle 14, for example, it was stated that they were resolute “*to empower the poor, particularly those living in remote, rural and marginalized urban areas, to access information and to use ICTs as a tool to support their efforts to lift themselves out of poverty*”<sup>2044</sup> to carry out the Millennium Development Goals.<sup>2045</sup> As noted above,<sup>2046</sup> this was further bolstered through a UNHRC Resolution in 2012, stating that the same human rights people had offline should also be protected online.<sup>2047</sup> Although the WSIS Principles noted that there had to be a “*global culture of cyber-security [which needed] to be promoted, developed and implemented*”<sup>2048</sup> and that “[i]t is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes...”,<sup>2049</sup>

---

<sup>2039</sup> Akindemowo, O.E. *The pervasive influence of anti-terrorist financing policy: post 9/11 non bank electronic money issuance* (2004) 19(8) *Journal of International Banking Law and Regulation* 289, 296-7.

<sup>2040</sup> Whitton, 17.

<sup>2041</sup> Fletcher Baldwin Jr, 138.

<sup>2042</sup> See in general regarding jurisdictional problems, Fletcher, N. *Challenges for regulating financial fraud in cyberspace* (2007) 14(2) *Journal of Financial Crime* 190, 198, 204.

<sup>2043</sup> *World Summit on the Information Society, Geneva 2003, Tunisia 2005* <<http://www.itu.int/net/osis/docs/geneva/official/dop.html>> accessed November 2016.

<sup>2044</sup> *ibid* Principle 14.

<sup>2045</sup> *ibid* Principle 2.

<sup>2046</sup> Section 7.2.2, *supra*.

<sup>2047</sup> A/HRC/20/L.13 *The promotion, protection and enjoyment of human rights on the Internet* (29 June 2012), Article 1.

<sup>2048</sup> *ibid* WSIS Principles, Principle 35.

<sup>2049</sup> *ibid* Principle 36.

there was no specific framework which countries could rely on in order to increase Internet access while giving them the capacity to inform and educate their citizens about the risk of cybercrime before it became an issue. Thus, any effectiveness to combat cybercrime is limited.

Saudi Arabia is a classic example of this problem. It now has a high Internet penetration, at 67.4% in 2016,<sup>2050</sup> equivalent to over 20million of its population,<sup>2051</sup> and a tripling of Internet access within ten years, from 19.5% Internet penetration in 2006.<sup>2052</sup> As outlined in chapter six,<sup>2053</sup> by increasing the population access to the Internet so quickly without the necessary capability to warn about cybercrime, Saudi has a high proportion of its Internet users who are vulnerable to cybercrime, with 6.5million users reporting that they were victims, ten percent higher than the global average.<sup>2054</sup> By combining the dangers of both poor Internet education with sudden Internet access, there are again gaps within international regulation in this area, providing the cybercriminal with a way of avoiding detection. Coupled with the emerging virtual currency market as noted above, countries with weaker or newer AML/CTF legislation are vulnerable to abuse by cybercriminals and terrorists using cybercrime as a way to finance their operations. Consequently, the UN's 1999 Convention and the FATF Recommendations become less effective in assisting international efforts to trace terrorist finances generated over the Internet. Again, this raises the question of Internet governance as a means of combating cybercrime, given some countries' difficulties in combating the problem.

---

<sup>2050</sup> Saudi Arabia *Internet Live Stats* (2016) <<http://www.internetlivestats.com/internet-users/saudi-arabia/>> accessed November 2016.

<sup>2051</sup> *ibid.*

<sup>2052</sup> *ibid.*

<sup>2053</sup> Chapter six, 6.4.

<sup>2054</sup> *ibid.*

Moreover, in 2008 the FATF published a report on the vulnerabilities of the Internet by criminals and terrorists, highlighting difficulties for financial institutions to trace suspicious transactions through several jurisdictions,<sup>2055</sup> suggesting that ISPs could have a role in monitoring transactions which are out of the ordinary to their customers' online behaviour.<sup>2056</sup> Additionally, the FATF report suggests that conflicting privacy legislation should be harmonised, to prevent problems with the collection of information by law enforcement agencies,<sup>2057</sup> and international cooperation to be formulated between states, financial institutions and ISPs.<sup>2058</sup> These are, of course, effective suggestions, however, without UN intervention into Internet governance, ISPs and jurisdictions are left with a complex system of bilateral treaties on information-sharing which do not necessarily address the inherent problems which are highlighted by cybercrime.

Finally, the WSIS in 2016 highlighted emerging threats to Internet users and law enforcement.<sup>2059</sup> In particular, WSIS noted that there were concerns about the Darknet and the need for it to be regulated, as well as deterrent provisions for cybercrime.<sup>2060</sup> Briefly, as noted in chapter five,<sup>2061</sup> cybercriminals are now using the TOR network to disguise their browsing history. A recent study highlighted that 57% of websites used on TOR were for illicit activity,<sup>2062</sup> showing that this is now the next

---

<sup>2055</sup> Financial Action Task Force *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (18 June 2008) [132] <<http://www.fatf-gafi.org/documents/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercial-websitesandinternetpaymentsystems.html>> accessed November 2016.

<sup>2056</sup> *ibid* [133].

<sup>2057</sup> *ibid* [134].

<sup>2058</sup> *ibid* [142].

<sup>2059</sup> United Nations World Summit on the Information Society *Forum Outcome Document* (2016), 244 <<https://www.itu.int/net4/wsis/forum/2016/Outcomes/#ft>> accessed November 2016.

<sup>2060</sup> *ibid*.

<sup>2061</sup> Chapter five 5.2.3. fn 253.

<sup>2062</sup> Moore, D. & Rid, T. *Cryptopolitik and the Darknet, Survival* (2016) Vol. 58 Iss. 1 <<http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>> accessed November 2016.

big threat for law enforcement authorities. Although outside the remit of this thesis, increasing knowledge of the Darknet and criminal marketplaces such as Silk Road<sup>2063</sup> have now highlighted that law enforcement has just scratched the surface of quickly changing technology and the manner in which cybercriminals and terrorists can use the web to mask their transactions. This further makes the point that Internet governance should be provided to the UN rather than a 'bottom up' approach, so that there is a more standardised approach by both ISPs and jurisdictions, to combat new threats as new encryption technologies surface.

## **7.5. Conclusion**

The events of 9/11 exposed a new set of difficulties for the international community. Terrorism is seen as one of the greatest dangers to modern society, because it eats away at society from within, perverting its institutions and governments as they react accordingly to the threat it poses.

Clearly, the UN reacted more gradually than the US and the UK to the use of the Internet by terrorist financiers since 9/11. While, in some respects, this is problematic, as there is still no set international standard to combating the use of the Internet by terrorists and differing interpretations of privacy, by being proactive rather than reactive, the UN can potentially balance the need for effective detection with the issue of privacy. However, even with its current system of compelling states to block and freeze terrorist assets, there is difficulty in enforcing equal standards, as many coun-

---

<sup>2063</sup> *United States of America v. Ross William Ulbricht a/k/a 'Dread Pirate Roberts', a/k/a 'DPR', a/k/a 'Silk Road'* 14-cr-68 (October 30, 2014).

tries do not have the technological advances or resources to enable their law enforcement agencies to carry them out. Furthermore, as the “*baseline*” for international efforts,<sup>2064</sup> it is imperative that present standards set by the FATF, and ultimately the UN, are equally applied. As Levitt states “...*without international co-operation, we are left with a patchwork of domestic, bilateral and regional efforts that at best work in parallel but not complimentary fashion, and at worst work at cross-purposes...*”.<sup>2065</sup>

Therefore, the effectiveness and appropriateness of international standards can be examined through a re-examination of the initial standards as set out in chapter one.

#### **7.5.1.        The effectiveness of international efforts to combat terrorist financing via the Internet**

It is key to revisit the first questions outlined in this thesis to be able to answer the question of effectiveness. Revisiting the aims of the 1999 Convention is critical to determine how effectively each example jurisdiction and, ultimately, international partners, have been in applying their overall requirements to combat terrorist financing. At a very basic level, the initial questions outlined in chapter one and addressed throughout the thesis can be narrowed down to one, in order to determine effectiveness:

*Have the aims of the 1999 Convention for the Suppression of the Financing of Terrorism been achieved when transposing them to Internet transactions?*

On the surface, this can be answered in the affirmative, as all countries have applied the 1999 Convention following 9/11, yet there are individual problems that

---

<sup>2064</sup> Levitt, 64.

<sup>2065</sup> *ibid* 62.



each example jurisdiction faces, which makes effectiveness less apparent. Furthermore, due to the lack of international regulations on governing the Internet and dealing with cybercrime, this leaves the opportunity to provide solutions to combat what is a patchwork of domestic and regional regulation - which helps terrorist financiers and hinders the work of those trying to disrupt their actions.

As outlined in chapter 1.4.1.1., the aims of the international community towards the financing of terrorism both before and after 9/11 can be summed up through the following:

- 1. An unequivocal condemnation of terrorism as criminal;*
- 2. All Member States to take steps to prevent and counteract, through domestic measures, financing of terrorism and terrorist organisations;*
- 3. International co-operation to prevent and suppress the financing of terrorism through criminalisation of terrorist financing, freezing and confiscating assets, as well as preventative measures;*
- 4. Adoption of regulatory measures to prevent and counteract movements of funds suspected to be intended for terrorist purposes;*
- 5. Intensifying and accelerating exchange of information concerning international movement of terrorist funds;*
- 6. Prosecution and punishment of perpetrators of terrorist financing.*

Going through each aim, it is difficult to see which of these have been implemented to their fullest extent, although it is clear that 9/11 ensured individual jurisdictions focused their efforts to deter and disrupt terrorist financing through applying the above aims. Granted, the first aim, an unequivocal condemnation of terrorism had, to a large part, been implemented since 9/11, with all member countries bound by Security Council Resolution 1373 to apply the 1999 Convention for the Suppression of the

Financing of Terrorism. Yet, as noted in 7.2.1, there is no clear definition of what constitutes ‘terrorism’, and, as a consequence, this nullifies the aim to criminalise terrorism, as some countries will inevitably have a wider version of what constitutes a terrorist act, such as Saudi Arabia, than other countries which have narrower definitions, such as the UK and the US. UN Security Council Resolution 1566 in 2004 did go further to condemn terrorism as a serious threat to peace, as well as provide an operational definition of terrorism as “*criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages with the purpose to provoke a state of terror in the general public or in a group of person or particular persons, intimidate a population or compel a government or international organisation to do or abstain from doing any act*”.<sup>2066</sup> Furthermore, such acts are “*under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic religious or other similar nature*”.<sup>2067</sup> However, this is still not a clear definition of terrorism, as it would take a General Assembly Treaty to ensure that the definition of terrorism is truly agreed upon, which will be outlined in further depth under 7.5.3. As a result, the unequivocal condemnation and criminalisation of terrorism, while on the surface, has been met through the adoption of the UN’s 1999 Convention and subsequent Security Council resolutions, without that definition, it is unclear whether this aim has been effectively met by all Member States.

Turning to the second aim of disrupting terrorist financing through domestic legislation, the UN’s initial aims were not met by all countries after 9/11. In particular, Saudi Arabia was unable to meet these obligations until 2010, a full 9 years after the

---

<sup>2066</sup> UN Security Council Resolution S/RES/1566 (2004) Creation of working group to consider measures against individuals, groups and entities other than Al-Qaida/Taliban, para. 3.

<sup>2067</sup> *ibid.*

events.<sup>2068</sup> This was not due to an effective enforcement strategy by the UN, but rather through peer-to-peer evaluation through the Financial Action Task Force which exposed the gaps in Saudi AML/CTF legislation, and was subsequently corrected by the Saudi authorities.<sup>2069</sup> In the US, primary counter-terrorist legislation rested upon viewing AML and CTF as a single crime,<sup>2070</sup> which has become wholly inadequate to combat two very different financial crimes. Additionally, while the UK had a battery of CTF legislation both pre- and post-9/11, this was rendered almost obsolete during 7/7 and the murder of Drummer Lee Rigby in 2013, due to the rising tide of ‘cheap terrorism’<sup>2071</sup> and the necessity to find other ways of combating terrorism and its financing. This requirement becomes more complex when dealing with terrorist financing generated over the Internet, as small transactions can be hidden through the sheer number of daily transactions made. While the Financial Action Task Force has adapted its research into new forms of terrorist financing and vulnerabilities emerging technology and issued guidance on new payment methods in 2013,<sup>2072</sup> it is still subject to ‘soft law’, or the voluntary participation of its members, rather than being a binding resolution for all countries to follow. Additionally, the recent identification by the World Summit on the Information Society of vulnerabilities of the Internet to terrorist financing,<sup>2073</sup> while useful, brings nothing new to the international community on combating this issue, or a legitimate, binding international framework to apply. Consequently, this second aim becomes ineffective due to the ever-evolving nature of terrorism and its financing, as well as the lack of a clear framework for countries to fall

---

<sup>2068</sup> Chapter six, 6.2.1.

<sup>2069</sup> *ibid.*

<sup>2070</sup> Chapter four, 4.3.2.

<sup>2071</sup> Chapter five, 5.3.2.

<sup>2072</sup> Chapter seven, 7.3.2 *supra*.

<sup>2073</sup> *ibid.*

back on to apply their laws effectively and uniformly, and leads onto problems applying the third aim on international co-operation to prevent and suppress the financing of terrorism.

This third aim is particularly important in the context of both terrorist financing and the application of these regulatory requirements onto finances generated and channelled through the Internet. Without the uniform or similar application of the previous two aims, the third aim becomes more difficult to undertake. By the very lack of a definition of terrorism, the ability to effectively and appropriately freeze assets without harming international relations between Member States becomes almost impossible, as some may not wish to co-operate should the individual not be determined as a terrorist suspect under their domestic interpretation of terrorism. Moreover, the case of HSBC and its dealings with both Iran and Mexican drug cartels, as outlined in chapter five,<sup>2074</sup> shows how problematic this aim becomes when financial institutions themselves seek to hide transactions which are considered under the 1999 Convention to be money laundering and terrorist financing. Even the fall-out to this revelation was not dealt with in a similar manner by the US and the UK - with the US seeking large fines from the bank, as well as criminal prosecutions to prevent further abuse of the financial system, and the UK asking for those charges to be dropped in 2012, due to considerations of the financial crash of 2008 and the delicacy of the financial markets within the UK.<sup>2075</sup> Essentially, the bank did not face similar charges in the UK,<sup>2076</sup> meaning that preventative measures become meaningless, due to the lack of enforcement. Therefore, again while this aim has been met on the surface, the case studies highlight that it becomes ineffective due to the lack of a uniform application

---

<sup>2074</sup> Chapter five, 5.3.2.

<sup>2075</sup> *ibid.*

<sup>2076</sup> *ibid.*

of the 1999 Convention. When applied to Internet Service Providers and Internet companies such as Google, Facebook and YouTube, the problem becomes more stark: they are not necessarily bound by international regulations in this area, therefore whatever actions they take on terrorist financing are either voluntary or regulated by domestic laws. They are not financial institutions per se, but they do enable the free flow of finances through their companies through subscription and advertising; consequently, they may not be caught by the 1999 Convention's aims, but may still be helping the flow of terrorist financing. As a result, the third aim becomes ineffective when applying it to some financing generated through the Internet.

HSBC's \$19bn involvement in the financing of terrorism<sup>2077</sup> can be further used as an example of where the fourth aim is rendered ineffective. While steps have clearly been taken by UN Member States since 9/11 to prevent and counteract movements of funds, the global nature of both the Internet and formal financial systems is not to be underestimated; hence the clear need for the 1999 Convention to somewhat harmonise countries' actions towards the disruption and prevention of terrorist financing from entering this international flow of finances. Not only had the bank's subsidiaries, HBUS and HSMX actively circumvented US sanctions by hiding transactions with countries such as Iran and North Korea, but the bank had resumed trading with a financial institution suspected of funnelling terrorist financing after 9/11, Al Rajhi Bank.<sup>2078</sup> Additionally, the backlog of the bank's own Suspicious Activity Reports, a key plank in the application of the 1999 Convention, was a factor in preventing these relationships from being revealed to authorities at an earlier stage.<sup>2079</sup> Therefore, the

---

<sup>2077</sup> Chapter five, 5.3.2 - HSBC's subsidiaries had hidden 28,000 suspicious transactions between 2001 and 2007, of which \$19.4bn had been channelled to Iran, at that time a proscribed state by the US Department of State.

<sup>2078</sup> *ibid.*

<sup>2079</sup> *ibid.*

aim of preventing the movement of funds is unable to be applied to the fullest extent; with the collusion of formal financial institutions which hold and transact billions of dollars daily, adopting regulatory measures to counteract their movement becomes more difficult to apply. Cybercrime is also a significant element in preventing this aim from being achieved to their fullest extent; given that the UN was silent on the use of computers for criminal purposes after 9/11, despite the broad wording of the 1999 Convention to include virtual currencies.<sup>2080</sup> By instead focusing on universal access to the Internet in the early 2000s<sup>2081</sup> without the associated frameworks to combat cybercrime and the use of the Internet by terrorist financiers, many countries who took advantage of higher proliferation rates simply did not have the resources to combat a growing criminal activity.<sup>2082</sup> Additionally, the rise of the ‘dark web’ means that, while more regulation is being placed on financial transactions which are carried out on the open web, local law enforcement and individual jurisdictions are less equipped to track transactions which have been generated and channelled through more illicit channels.<sup>2083</sup> As a result, even though the basic tools to combat terrorist financing through virtual currencies are present within international legislation, individual jurisdictions are hampered by their own sovereignty to counteract a global crime because there is no UN instrument to combat cybercrime. By comparison, the European Convention on Cybercrime 2001 does specifically combat cybercrime and crimes against the computer and provides the minimum standards required to ensure international co-operation. By accepting this international instrument, the fourth aim could be achieved.

The fifth aim - that of accelerating the exchange of information - is also subject

---

<sup>2080</sup> Chapter seven, 7.4. *supra*.

<sup>2081</sup> *ibid*.

<sup>2082</sup> *ibid*.

<sup>2083</sup> *ibid*.

to some hurdles. Usually, there are bilateral and multilateral agreements between countries to further this aim; for example, the “Five Eyes” partnership of the US, UK, Australia, Canada and New Zealand and the TEMPORA system of Internet intelligence-gathering is an extreme example of the open exchange of information as mentioned in chapter five, including that of individuals from states outside its membership.<sup>2084</sup> Furthermore, EUROPOL relies on shared information to capture the movement of funds between EU Member States and to capture terrorists who are moving between European cities, such as the Paris bomber Salah Abdeslam, who was caught in Belgium through vital information sharing.<sup>2085</sup> However, when the requirements of the 1999 Convention have to be met - for example, Suspicious Activity Reports made by financial institutions on suspicious transactions which could be money laundering or terrorist financing - the sheer scale of reporting means that formal financial institutions and subsequently individual countries’ Financial Intelligence Units which receive this information are inevitably behind the almost immediate flow of terrorist financing via the Internet. This is exemplified by the weight of Suspicious Activity Reports received by the US and the UK - with over a million and a half lodged with both jurisdictions in 2014-15. It is telling that Donohue notes “*white noise [is] created by the deluge of data increas[ing] the difficulty of ferreting out real threats*”.<sup>2086</sup> Yet, as noted in 7.3.2., conversely, Saudi Arabia has significantly under-reported its suspicious transactions, with formal financial institutions lodging only 1967 by 2014<sup>2087</sup> and just 126 terrorist financing STRs being submitted.<sup>2088</sup> This wealth of difference

---

<sup>2084</sup> Chapter five, 5.1.2.a.

<sup>2085</sup> *ibid* Chapter five, 5.2.3.

<sup>2086</sup> Donohue, L. K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int’l L 303, 395.

<sup>2087</sup> Saudi Arabia Financial Intelligence Unit *Annual Report 2014* (Ministry of the Interior), 18 <<https://www.moi.gov.sa/wps/portal/Home/sectors/safiu>> accessed November 2016.

<sup>2088</sup> *ibid* 22.

means that there are significant difficulties when sharing information which cannot be discovered in time for authorities to act and prevent the flow of terrorist financing. While there has been impetus for UN Member States to share information since 9/11, the patchy application of the 1999 Convention shows the inability to cleanly divulge important information which should prevent a terrorist attack.

Finally, the aim of prosecuting and punishing the perpetrators of terrorist financiers is of paramount importance and links each and every one of the previous aims before it. Essentially, the international aim is to keep terrorists from being able to carry out their acts and to prevent them from recruiting others in the future. However, the reality of difficult evidence-gathering to effectively prosecute offenders who have raised financing via the Internet is no more evident than in the UK. As noted in chapter five, s.17 of the Regulation of Investigatory Powers Act explicitly prohibits the use of intercepted communications as evidence in court, meaning that a powerful tool to prosecute terrorists is essentially nullified,<sup>2089</sup> in comparison to other common law countries such as the US, which routinely uses intercept evidence.<sup>2090</sup> This obvious lacuna of a leading Member State in its fight against terrorist financing clearly prevents the overarching aim from being fully applied. Additionally, the secrecy of Saudi Arabia's terrorism courts means that it is difficult to assess whether their prosecutions are for the conviction of terrorists and their financiers, or if there are other dissenters of the regime who are caught by counter-terrorist provisions.<sup>2091</sup> Consequently, the final aim is not fully realised by the Member States examined within this thesis.

---

<sup>2089</sup> Chapter five, 5.1.2.a.

<sup>2090</sup> *ibid.* At a federal level, intercept evidence gathered under Title III of the Omnibus Crime Control and Safe Streets Act 1968 can be routinely disclosed under testimony in criminal cases – see 18 U.S.C. §2517(3). Furthermore, §203 of the USA PATRIOT Act 2001 (Pub. L. 107-56, 115 Stat. 272) enhances existing disclosure rules and applies them to criminal cases involving terrorism.

<sup>2091</sup> Chapter six, 6.2.2.



### 7.5.2            **The appropriateness of international efforts to combat terrorist financing via the Internet**

All three example jurisdictions have used terrorism and national security as reasons to shield themselves from what are inappropriate techniques of surveillance and methods of tracing terrorist finances through Internet communications in a period of what is, essentially ‘peace time’. Revisiting the initial points made within the introduction, appropriateness can be measured by combining existing domestic legislation, as well as three main areas of both the 1999 Convention for the Suppression of the Financing of Terrorism and the 2000 European Convention on Cybercrime:

1. *Article 15 of the 1999 Convention on extradition and mutual legal assistance;*
2. *Article 17 of the 1999 Convention on subjects taken into custody and subject to proceedings;*
3. *Article 15 of the Cybercrime Convention on the application of domestic powers.*

While, as mentioned previously within this chapter,<sup>2092</sup> the International Convention on Human Rights is non-binding on Member States, the first two Articles by virtue of Security Council Resolution 1373, are. Significantly, Article 15 makes reference to certain human rights which can be transferred onto the investigation of terrorist financing through the Internet, including that countries can refuse legal assistance or extradition on the basis of preventing punishment because of race, religion, nationality, ethnic origin and political opinion - thus potentially capturing the appropriateness of using powerful censorship or surveillance tools to combat terrorist financing on the basis of freedom of speech and freedom of expression. Additionally, Article 17 states that those who are taken into custody or is subject to proceedings should be guaranteed fair treatment including the enjoyment of international human

---

<sup>2092</sup> Chapter seven, 7.2.2. *supra*.

rights law - including right to a fair trial. None of the example countries have made specific reservations or derogations on Articles 15 and 17 of the Convention, therefore on this basis, all three countries could have inappropriately used their techniques to trace terrorist financing over the Internet.

The third area, those of human rights derived from the Cybercrime Convention, can ultimately be used for two out of the three example jurisdictions outlined within this thesis. Therefore, both the UK and the US, by having signed and ratified that Convention, must take into account the human rights which are reflected in Article 15, which includes proportionality of measures to tackle cybercrime. The assessment made of both countries therefore not only use their own courts' interpretation of domestic human rights but also that of international legislation on human rights.

#### **7.5.2.1. The United States**

As mentioned within chapter one, the relevant US civil rights relating to counter-terrorist financing and Internet transactions are those of privacy, freedom of expression and the right to a public trial.<sup>2093</sup> The problem for the United States (US) has been the speed at which its key domestic legislation to combat terrorism and its financing, the USA PATRIOT Act of 2001, had been passed in the wake of 9/11. The most controversial elements of the Act when assessing its use since 9/11 - that of the surveillance measures under Title II - were subject to sunset clauses, but these were continually re-approved by Congress.<sup>2094</sup> Specifically, regarding appropriateness within the US's own domestic legislation, the use of 'pen and trap' registers, which harnessed the entire contents of email communications, has been consistently criticised as breaching

---

<sup>2093</sup> Chapter one, 1.4.2.2.

<sup>2094</sup> Chapter five, 5.2.2.

the US Constitution's own Fourth Amendment on the individual's right to privacy.<sup>2095</sup> Furthermore, the use of the Foreign Intelligence Surveillance Acts of 1978 and 2008 on stored international communications has little judicial oversight with warrants being assessed by a private Foreign Intelligence Surveillance Court, again raising concerns about the right to a public trial, a civil right enshrined within the Sixth Amendment.<sup>2096</sup> These concerns about the appropriateness of the US's intelligence measures came to a head when Edward Snowden, a former National Security Agency operative, revealed details of trans-Atlantic Internet data capture programmes, PRISM and TEMPORA, whereby both UK and US intelligence agencies carried out mass surveillance on their own citizens' email and Internet communications, raising the possibility that, in the US at least, it was unconstitutional.<sup>2097</sup>

Turning to the international requirements, the US, while overall maintaining the ideals of freedom of expression and having a court system which is able to openly challenge the constitutionality of some of its counter-terrorism laws, has overstretched its use of what is emergency legislation to employ large-scale surveillance techniques against its own citizens and others based outside of the US. Although there have been moves to tighten regulations on its own citizens, because the largest ISPs and Internet companies are based in the US and are therefore bound by US law, the question of mutual legal assistance with countries whose citizens have been captured by their surveillance techniques and extradition is of some concern. Without the necessary assurances to keep their citizens' communications private, the US has in the past cooled international relations - most significantly with the European Union Parliament when it was found in 2006 that the SWIFT banking database was being routinely harvested

---

<sup>2095</sup> *ibid.*

<sup>2096</sup> *ibid.*

<sup>2097</sup> *ibid.*

for financial information on European citizens by the US law enforcement authorities.<sup>2098</sup> This, the Parliament maintained, was a breach of its data protection laws and, although agreement was eventually reached over access to the database, the effects of being unable to balance effective counter-terrorism tools with privacy can have significant international effects.<sup>2099</sup>

Taking both domestic and international concerns about the US's tactics on counter-terrorist financing and Internet data together, it is therefore clear that the US not only breached its own domestic civil liberties of privacy and right to a public trial, but also overstepped its role in international affairs.

#### **7.5.2.2. The United Kingdom**

Unlike the US, the United Kingdom (UK) is held to a higher standard of appropriateness, not only because it signed and ratified the Convention on Cybercrime, but it also incorporated into its domestic law the Universal Declaration of Human Rights via the European Convention on Human Rights, with specific legislation aimed at privacy, freedom of expression and the right to a fair trial.<sup>2100</sup> Under the Human Rights Act 1998, these have been held as safeguards to protect appropriateness when successive UK Governments have applied counter-terrorist financing legislation, as well as their own surveillance techniques to capture illicit finances. Therefore, it has been challenged more significantly than, for example, the US and Saudi Arabia over its use of surveillance and data capture, especially within the regional courts of the European

---

<sup>2098</sup> Chapter four, 4.3.2.

<sup>2099</sup> *ibid.*

<sup>2100</sup> Chapter five, 5.2.1. - s.10 Human Rights Act 1998 c.42 on freedom of expression; chapter five, 5.2.2 a.- s.6 Human Rights Act on the right to a fair trial; chapter five 5.2.2.a. - s.8 of the Human Rights Act 1998 on the right to privacy.

NB. All of these sections correlate with the European Convention on Human Rights Articles.

Court of Human Rights and the Court of Justice of the European Union.<sup>2101</sup> Yet, the UK still pushes the boundaries of acceptability, proportionality and appropriateness when it applies its counter-terrorism legislation.

As noted above, the involvement of UK's intelligence agency, GCHQ in the trans-Atlantic data harvesting of Internet communications via TEMPORA, re-evaluated the notion of data privacy in light of both the threat of terrorism and the data protection rules the UK is bound by. While the UK was acting in accordance with its domestic legislation, the Regulation of Investigatory Powers Act 2000, as well as the EU Data Retention Directive, the appropriateness on the wider scale within the European Union was and still is challenged after a significant ruling by the Court of Justice of the European Union in *Digital Rights Ireland*,<sup>2102</sup> which ruled that the EU's Data Retention Directive was invalid due to data protection and privacy concerns.<sup>2103</sup> Yet the UK is still attempting to get around this ruling, through the Investigatory Powers Act 2016, which re-enacted many of the Directive's provisions.<sup>2104</sup> Undoubtedly, there will be cases before the European Court of Human Rights and the Court of Justice of the European Union about the appropriateness of this Act, which has, thus far done little to assuage concerns about freedom of expression and privacy.<sup>2105</sup> While the US and the EU have moved towards further privacy protection, the UK is using

---

<sup>2101</sup> E.g. *Handyside v UK* App. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737 on freedom of expression (chapter 5.2.1.); Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post -och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis* (C-698/15), 19 July 2016 on bulk metadata collections and the retention of data for the purposes of law enforcement.

<sup>2102</sup> C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others. Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung* (C-594/12), *Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221; chapter 5.2.2.b.

<sup>2103</sup> *ibid.*

<sup>2104</sup> Chapter five, 5.2.3.

<sup>2105</sup> Chapter five, 5.2.3.a and 5.2.3.b.

national security to enable it to circumvent its more recent obligations.<sup>2106</sup> The appropriateness again would have to be seen through the international provisions contained within the 1999 Convention and the Convention on Cybercrime. Upon closer inspection, the fact that the UK's intelligence services have been found to have breached the fundamental principles of the European Union towards the Internet - that of data protection and privacy - is unlikely to have an impact on the mutual legal assistance and extradition given that the UK is currently a member. Yet, it still leaves the UK's actions since 9/11 open to significant legal challenge on the basis of its inappropriateness, and may also affect its relationship with countries outside of the EU, which also hold equally high standards of data protection and privacy.

#### **7.5.2.3. Kingdom of Saudi Arabia**

While the UK must be held to a higher standard of appropriateness, by the very nature that it has enshrined significant human rights into its own blackletter law and is bound by the legislation of the European Union, the Kingdom of Saudi Arabia's appropriate actions must be assessed at a lower standard because it has no equivalent promise to its citizens. The Constitution of Saudi Arabia, however, does have some principles of privacy for communications under Article 41, which notes that "[t]elegraphic, postal, telephone, and other means of communications shall be safeguarded. They cannot be confiscated, delayed, read or listened to except in cases defined by statutes."<sup>2107</sup> However, even here there is a stretching of the interpretation of the Constitution's aims, as

---

<sup>2106</sup> Under Article 8(2) of the European Convention on Human Rights, this provides authorities with the exemption of national security measures when considering the right to privacy - see chapter five, 5.2.2.

<sup>2107</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 41 <[http://www.parliament.am/library/sahmanadrutyunner/Saudi\\_Arabia.pdf](http://www.parliament.am/library/sahmanadrutyunner/Saudi_Arabia.pdf)> accessed 12 April 2018.

well as the principles of Shari'ah to prevent spying and invasion of privacy,<sup>2108</sup> when it is almost taken for granted that monitoring of the content of communications is carried out by Saudi authorities on a regular basis because there is no independent data controller to monitor the use of data, unlike the US and the UK.<sup>2109</sup> This also extends to the Saudi principles of financial confidentiality, contained within Article 8 of the Anti-Money Laundering Law 2003, where it is unclear, again due to the lack of a data controller, that there have been significant breaches of this law by Saudi authorities. As such, it is therefore concluded that some of Saudi Arabia's actions surrounding privacy - as with the UK and the US - have been inappropriate since 9/11.

While it is arguable that the Saudi authorities are acting well within their sovereignty and remit because the Universal Declaration of Human Rights is non-binding, the 1999 Convention at Article 15 again states that there should be no obligation to afford mutual legal assistance or extradition where the request has been made for the purpose of prosecuting an individual for, amongst other areas, political opinion. Therefore, freedom of expression should be taken into account when assessing whether Saudi Arabia has been appropriate in its conduct towards individual actors such as Raif Badawi, whose website called for a day of discussion with Saudi liberals and who was subsequently punished for 'insulting Islam' because of his online communications.<sup>2110</sup> His punishment is well within the Saudi Constitution, which states at Article 39 that information, "publication and all other media shall employ courteous language and the state's regulations and they shall contribute to the education of the

---

<sup>2108</sup> 49:12 Qur'an: *O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other. Would one of you like to eat the flesh of his brother when dead? You would detest it. And fear Allah; indeed, Allah is Accepting of repentance and Merciful* <<https://quran.com/49:12>> accessed November 2016.

<sup>2109</sup> Chapter six, 6.2.2.

<sup>2110</sup> Chapter six, 6.2.1.

nation and the bolstering of its unity” and calls for the prohibition of acts that “foster sedition or division or harm”.<sup>2111</sup> Yet, whether this fits with the overall picture of freedom of expression through political opinion, as alluded to within the 1999 Convention, is less positive, and therefore it can be said that such actions - as with the UK and the US - could harm the free flow of information between countries with high levels of Internet control, and those with more of a focus on the privacy of information and freedom of expression. Therefore, by the very point that Saudi Arabia could be harming its own ability to receive such assistance because of its stance on human rights inevitably leads one to the conclusion that they would be inappropriate from other countries’ viewpoints, even if they are carried out within the sovereign laws of the country.

#### **7.5.2.4. The United Nations and other international organisations**

Because of the UN’s reluctance to set out a clear international framework on the regulation of Internet surveillance to track such terrorism-related transactions,<sup>2112</sup> as well as the absence of a single definition of terrorism,<sup>2113</sup> Member States are left to define what they believe is an appropriate use of government tools. The 1999 Convention alludes to human rights, but still does not specifically bind Member States to setting out an appropriate course of balancing an effective way of using surveillance with the rights of privacy and freedom of expression. This leads to an unequal application of the Convention, meaning that even countries with more stringent standards of human

---

<sup>2111</sup> Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005), Article 41 <[http://www.parliament.am/library/sahmanadrutyunner/Saudi\\_Arabia.pdf](http://www.parliament.am/library/sahmanadrutyunner/Saudi_Arabia.pdf)> accessed 12 April 2018.

<sup>2112</sup> Chapter seven, 7.2. *supra*.

<sup>2113</sup> Chapter 7.2.1. *supra*.



rights still stretch their powers to the very limit of what would be acceptable in ordinary circumstances, as well as using national security as a way of circumventing those rights which have often been placed into blackletter law or enshrined within their constitutions. Essentially, all the example countries set out above have worked within the remit of their respective laws, with a strict interpretation of their actions concluding them ‘appropriate’, yet they potentially damage international mutual assistance under the 1999 Convention because some may view others’ actions as inappropriate or breach the human rights of their subjects.

Additionally, the treatment of charities across all three example jurisdictions through asset freezing provisions has been of some concern. Again, while each has worked within their own sovereign remit, as well as the requirements of the 1999 Convention, the effects of the Convention’s asset-freezing provisions on charities has been stark. For example, Muslim charities were routinely targeted by the US, causing some charities to cease operations altogether and leading to claims that the actions undertaken since 9/11 have breached the First Amendment of the US Constitution on freedom of religion.<sup>2114</sup> Furthermore, the US case of *KindHearts*<sup>2115</sup> showed that local courts had been ‘arbitrary’ when applying freezing orders.<sup>2116</sup> In the UK, similar concerns have been raised, including the effects on legitimate humanitarian organisations working in war zones to provide aid. Yet, while steps had been taken by the UK to assist charities in this situation to make asset freezing measures more appropriate,<sup>2117</sup> the Government had not provided any guidance to charities and Non-Governmental

---

<sup>2114</sup> Chapter four, 4.3.1.

<sup>2115</sup> *KindHearts for Charitable Humanitarian Development Inc v. Timothy Geithner et al.* Case 3:08-cv-02400 (18 August 2009).

<sup>2116</sup> *ibid* chapter five, 5.3.1.

<sup>2117</sup> Chapter four, 4.3.1.; s.17 of the Terrorist Asset Freezing Act allowed humanitarian organisations and NGOs to apply for licences which would allow them to withdraw financing in certain situations.

Organisations working in high risk zones to be able to take advantage of them.<sup>2118</sup> Furthermore, financial institutions continue to block some legitimate charities' donations, meaning that millions of pounds of donations are foregone.<sup>2119</sup> Consequently, the overarching framework on asset freezing and monitoring charities, while necessary in the wake of the 9/11 Commission's findings on the proliferation of charities by terrorist financiers, may cause unintended consequences for those legitimate charities which have been effectively 'tarred with the same brush' as terrorist organisations.

Conversely, the UN's own Human Rights Council has been far more proactive in the area of appropriateness, assessing whether large scale surveillance operations or website filtration carried out by the example countries is compatible with the Universal Declaration of Human Rights and appointing its own Special Rapporteur to examine each countries' privacy laws.<sup>2120</sup> However, its work is hampered by the simple fact that its resolutions are non-binding. Consequently, while there are options for countries to balance the appropriateness of their techniques to capture terrorist communications via the Internet, there is no such impetus to make these binding.

### **7.5.3. Suggestions for reform**

Clearly, by the very nature of a lack of international regulation, there have been gaps within the application of domestic law and inherent problems when applying the 1999 Convention's aims to Internet transactions. Therefore, below are suggestions to enhance the effectiveness and appropriateness of capturing terrorist financing via the Internet and ultimately achieve the final aim of the 1999 Convention: punishing and prosecuting offenders to deter further acts from occurring. This section is therefore

---

<sup>2118</sup> *ibid* chapter four, 4.3.1.

<sup>2119</sup> *ibid*.

<sup>2120</sup> Chapter seven, 7.2.2. *supra*.

split into two sections; improvements to domestic law and improvements to international law. Firstly, the three individual countries can learn from each other's innovations in order to increase their effectiveness and appropriateness and secondly, the UN's actions can be increased to ensure that a more equal application of terrorist financing and Internet communications can be made in future.

#### **7.5.3.1. Improvements to domestic law**

So that jurisdictions are able to cope with the rising tide of both digital technology and the ability of terrorist organisations or criminals to subvert the Internet for their personal gains, below are some suggestions for each jurisdiction to be able combat terrorist financing through the Internet both effectively and appropriately. The US, throughout this thesis has been criticised for one fundamental flaw in its 'War on Terror': that of failing to recognise the differences between money laundering and terrorist financing through its anti-terrorism legislation. Thus, a simple solution would be to look towards the UK's existing legislation which relies less on money laundering techniques. Furthermore, the UK should be looking at how to improve the effectiveness and appropriateness of its legislation, including the introduction of intercept evidence in court, refining its website filtration and surveillance techniques to become more in line with its counterparts, the US and the European Union, as well as looking towards innovative techniques to prevent radicalisation over the Internet, such as those undertaken in Saudi Arabia. Finally, Saudi Arabia, with its proximity to ISIL's territory and sharp rise in Internet proliferation, should be considering specific cybercrime laws to combat the increasing technological advances of terrorist financiers who commit cybercrime and further their aims.

**7.5.3.1.a. The United States: Separating Anti-Money Laundering from Counter-terrorist Financing**

As noted above<sup>2121</sup> and within chapter four,<sup>2122</sup> the US had relied upon its existing anti-money laundering (AML) legislation to combat terrorist financing, meaning that it viewed the criminal offences as similar.<sup>2123</sup> Yet, this has been a fundamental flaw in the US's reaction to counter-terrorist financing (CTF) via the Internet; including using Suspicious Activity Reports submitted by financial institutions, companies and charities to Financial Intelligence Units to track and trace terrorist finances. As will be elaborated on further in 7.5.3.2.b. whereas Suspicious Activity Reports are based on knowledge of patterns of suspicious behaviour upon which computer algorithms can be created to easily detect money laundering, terrorist financing can also use legitimate finances as well, meaning that rather than hiding money, it is often in plain sight.<sup>2124</sup> As noted in chapter four,<sup>2125</sup> Donohue mentions that “...*it is difficult, if not impossible, to discern patterns in financial transactions that would signify terrorist activity...*”.<sup>2126</sup> This is just one example where AML provisions are unable to adapt to the aims of CTF or the concept that both are entirely separate crimes.

Consequently, the US should consider the UK's stance on CTF, recognising it as a separate crime. This would, no doubt, increase the effectiveness and appropriateness of the US's stance on CTF and reduce the problems its Financial Intelligence Units, as well as financial institutions, have in recognising certain behaviour which

---

<sup>2121</sup> Chapter seven, 7.5.1. *supra*.

<sup>2122</sup> Chapter four, 4.3.2. *supra*.

<sup>2123</sup> *ibid*.

<sup>2124</sup> Chapter four, 4.3.2.

<sup>2125</sup> *ibid*.

<sup>2126</sup> Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008), 345 – who also mentions that the Financial Action Task Force also reached the same conclusion in 2002; chapter 4.3.2.

would denote terrorist financing amongst the millions of daily Internet transactions. Within chapter four, it was suggested that it may, instead be more effective if law enforcement authorities co-operate with financial institutions to increase the speed at which they receive transaction records of suspected terrorists to trace them before a terrorist act is committed.<sup>2127</sup> This, as surmised by Roth et al, is already a viable option under §314 of the PATRIOT Act, this is already a viable option, which the FBI already uses for emergencies.<sup>2128</sup> As a result, by amending its existing legislation on counter-terrorist financing, the USA PATRIOT Act, to recognise counter terrorist financing as a separate predicate offence, the US can increase the effectiveness of its battery of counter-terrorism legislation.

#### **7.5.3.1.b. The United Kingdom: using intercept evidence in court**

As highlighted in 7.5.1.2 above, as well as chapter five,<sup>2129</sup> this is a significant gap within the UK's actions to effectively punish and prosecute offenders of both terrorism and terrorist financing over the Internet. The UK is the only common law country in the world to ban intercept evidence from being used in court, which not only increases the ineffectiveness of counter-terrorism trials but is also inappropriate.<sup>2130</sup> As new technologies are increasingly being used as evidence as to the intent of the alleged

---

<sup>2127</sup> Chapter four, 4.3.2. outlining the suggestions of Roth et al. on treating counter-terrorist financing differently.

<sup>2128</sup> Roth, J. Greenberg, D. Wille, S. *National Commission on Terrorist Attacks Upon the United States Staff Monograph on Terrorist Financing* (2004) 59-60 <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018; chapter four, 4.3.2.

<sup>2129</sup> Chapter five, 5.2.2.a.

<sup>2130</sup> Both Liberty and Justice, two human rights organisations, that intercept evidence ensures a fair trial under Article 6 of the European Convention of Human Rights because the prosecution currently has the advantage of knowing of the evidence, yet the defence has no right to challenge it in open court; Carlo, S. *5 Reasons why we need intercept evidence in court* (Liberty Blog, 26 February 2016) <<https://www.libertyhumanrights.org.uk/news/blog/5-reasons-why-we-need-intercept-evidence-court>> accessed November 2016.

perpetrator, the UK's unilateral ban seems all the more archaic and outdated. As Lord Lloyd of Berwick, who was in charge of an evaluation on intercept evidence noted, there was difficulty in obtaining evidence to charge and convict terrorists, especially those involved in planning and directing terrorists acts without being present at the point of execution.<sup>2131</sup> This statement doubtless includes those who are financing terrorism or directing donations from the other end of a computer. Consequently, through using intercept evidence, UK courts would not only be able to use further information to deliberate whether a criminal offence has been committed, but also allow defence teams to challenge the information gathered against the defendant. By allowing intercept evidence to be heard in an open court, and to place all retained information on a suspect at the discretion of the courts, Article 6 would not be compromised, as backed by the civil liberties organisations, JUSTICE.<sup>2132</sup> This would also make the UK's assessment of intercept evidence align with Article 6 of the European Convention on Human Rights - the right to a fair trial - as there would be no need to use control orders or secret inquiries.<sup>2133</sup> To do so would be a clear step towards achieving an aim of the international community towards counter-terrorist financing and be an appropriate form of prosecuting individuals with evidence gained from electronic surveillance. Furthermore, it would equalise the ability of the UK's justice system with those of other common law countries to effectively convict those who are guilty of terrorist financing via the Internet.

#### **7.5.3.1.c. The United Kingdom: Balancing surveillance with privacy**

As alluded to throughout this thesis, each example country has its own difficulties in

---

<sup>2131</sup> *ibid.*

<sup>2132</sup> Chapter five, 5.2.2.a.

<sup>2133</sup> *ibid.*

applying effective and appropriate surveillance and website filtration techniques which would capture terrorist financiers' communications while balancing privacy and freedom of expression. Yet, because the UK is a member of the European Union, which has strong data protection laws, and has incorporated international human rights into blackletter law, it should be held to a higher standard. This becomes more relevant - as mentioned in 7.5.2.2. above - when the UK lays itself open to challenge within its own domestic courts, as well as those of the European Union and the European Court of Human Rights. Therefore, the UK must refine its surveillance techniques to become more robust, as well as provide international best practice in this area.

As such, on the issue of website filtration, the UK should reconsider its actions to date as, without an effective legislative framework, its 'opt in' form of website filtration could be open to abuse due to the fact that it leaves Internet Service Providers to decide which websites should be blocked.<sup>2134</sup> Furthermore, as noted earlier,<sup>2135</sup> it could face challenge within the European courts on the basis that it breaches freedom of expression.<sup>2136</sup> Consequently, by requiring ISPs to monitor website content with a strict set of legislative guidelines to ensure that they can programme blocking technology legally and ethically, this would provide part of the solution to increase effectiveness and balance it with appropriateness. This must also be backed by independent oversight through a judicial tribunal to ensure that neither the ISPs nor governments abuse this power. Such a step would doubtless bring the UK into line with both US and European Union stances on website filtration.

Moreover, the UK can increase the appropriateness and effectiveness of its

---

<sup>2134</sup> Chapter five, 5.2.1.

<sup>2135</sup> *ibid*; Chapter seven, 7.5.2.2. *supra*.

<sup>2136</sup> *ibid*.

position on the surveillance of communications to capture terrorist financing through emails and social media messages. At present, the UK's Investigatory Powers Act depends upon two strands of surveillance - that of Internet data retention by Internet Service Providers and bulk data collection by security services. This continuance of two areas which had been of controversy through the UK's TEMPORA programme - albeit with additional safeguards<sup>2137</sup> - places it in direct conflict with the European Union's stance in *Digital Rights Ireland*.<sup>2138</sup> Furthermore, the Act's position of collecting data on Internet Connection Records, which can track individuals' web history, as well as mobile apps and logs of any other device which was Internet-connected, including games consoles, digital cameras and e-book readers,<sup>2139</sup> has been rejected by other countries such as the US, Canada, Australia and Germany,<sup>2140</sup> meaning that mutual legal assistance under Article 15 of the 1999 Convention could be compromised.

Therefore, some of the recommendations from David Anderson QC, the Independent Reviewer of Terrorism Legislation, should be assessed by the UK Government to ensure that its counter-terrorism legislation is compatible with data protection requirements from the EU and becomes more effective in finding terrorist communications within the mass of Internet conversations which happen daily. For example,

---

<sup>2137</sup> Chapter five, 5.2.3.

<sup>2138</sup> Chapter five, 5.2.3.

<sup>2139</sup> Liberty *Liberty's written evidence on the Investigatory Powers Bill* (March 2016), 22 paras. 43-44 – the only exception is local authorities - <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018.

<sup>2140</sup> Chapter five, 5.2.3.



bulk collection of data should be subject to strict additional safeguards, including judicial authorisation,<sup>2141</sup> a tighter definition of the purposes for which a bulk warrant is sought,<sup>2142</sup> a targeting of communications of persons believed to be outside the UK,<sup>2143</sup> as well as a specific interception warrant to be judicially authorised if the applicant wishes to look at communications of a person believed to be within the UK.<sup>2144</sup> Accepting these recommendations, made after the revelations of Edward Snowden, would mean that the UK has a more appropriate standard of surveillance which would be compatible with other European Union Member States. Furthermore, as outlined in the initial judgement of *Secretary of State for the Home Department v Tom Watson et al.* the use of retained data must be ‘strictly necessary’ in the fight against serious crime, that is, no other measure or combination of measures could be as effective,<sup>2145</sup> and must include all of the safeguards described in *Digital Rights Ireland*. Most importantly, the UK’s legislation or regulation for retained data must be proportionate,<sup>2146</sup> meaning that the serious risks to privacy and data protection of the majority of law abiding citizens must not be disproportionate to the significant advantages of data retention in the fight against serious crime.<sup>2147</sup> By taking on the above recommendations of the Independent Reviewer of Terrorism Legislation and the Court of Justice of the European Union, the UK’s legislative response to terrorist communications will ultimately become more robust.

---

<sup>2141</sup> *ibid* Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015), Recommendation 22, Chapter 5, 5.2.3.a. <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018.

<sup>2142</sup> *ibid* Recommendation 43.

<sup>2143</sup> *ibid* Recommendation 44.

<sup>2144</sup> *ibid* Recommendation 79.

<sup>2145</sup> *Opinion by Henrik Saugmandsgaard ØE Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB v Post -och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15)*, (19 July 2016); Chapter five, 5.2.3.a.

<sup>2146</sup> *ibid*.

<sup>2147</sup> *ibid*.

#### **7.5.3.1.d. The United Kingdom: Using innovation to capture acts of cheap terrorism**

In chapter five,<sup>2148</sup> and the conclusion above<sup>2149</sup> it was clearly outlined that, while the UK recognised the dangers of ‘cheap terrorism’, the difficulties in applying subsequent initiatives, including its Prevent programme to radicalisation over the Internet were apparent. Specifically, the infiltration of the Prevent programme by extremist groups who received funding,<sup>2150</sup> as well as the lack of the programme’s reach to young people who were radicalised by extremist groups over the Internet,<sup>2151</sup> clearly highlighted gaps within the Prevent programme. Additionally, the appropriateness of the programme has been severely criticised on the basis of its focus on one sector of the community,<sup>2152</sup> as well as poor training of public sector employees who have to identify and refer individuals to the programme.<sup>2153</sup> As a result, not only is more training required to ensure that public sector employees are trained sufficiently, but also innovative ways to combat extremist Internet communications from reaching those who are at risk of radicalisation from all sections of UK society.

Therefore, it is worth considering Saudi Arabia’s ‘Sakinah’ Campaign by the Ministry of the Interior, which tracks communications from terrorism-affiliated websites and infiltrates them to prevent radicalisation,<sup>2154</sup> providing one-to-one chats with

---

<sup>2148</sup> Chapter five, 5.3.2.

<sup>2149</sup> Chapter seven, 7.5.1.

<sup>2150</sup> *ibid.* Chapter five, 5.3.2.

<sup>2151</sup> *ibid.* E.g. A 15 year old boy was sentenced to life imprisonment for inciting terrorism overseas; Crown Prosecution Service *15 year old jailed for part in international terror plot* (2 October 2015) <[http://www.cps.gov.uk/news/latest\\_news/15\\_year\\_old\\_jailed\\_for\\_part\\_in\\_international\\_terror\\_plot/](http://www.cps.gov.uk/news/latest_news/15_year_old_jailed_for_part_in_international_terror_plot/)> accessed November 2016.

<sup>2152</sup> *ibid.* Chapter five, 5.3.2.

<sup>2153</sup> *ibid.*

<sup>2154</sup> Chapter six, 6.2.1.

those who are seeking out terrorism.<sup>2155</sup> As outlined in chapter six, Sakinah is officially a non-governmental organisation, which provides ways to diffuse potential radicalisation.<sup>2156</sup> This has proven to be quite successful as some of the volunteers are former extremists who have been turned around by the programme.<sup>2157</sup> This is confirmed by an article subsequent to this thesis by al-Saud, who explains that a collection of individuals from religious, psychological and social disciplines target social media and online forums to confront extremist views,<sup>2158</sup> using a database of theological reasoning and arguments on topics which are expressed through extremism.<sup>2159</sup> This, as al-Saud noted, has not been limited to citizens Saudi Arabia alone, but has also reached individuals as far away as Europe and the US through its website.<sup>2160</sup> A similar programme which simultaneously collects information and provides one-to-one help online to those who have been radicalised may be a worthwhile route. Clearly, consideration of privacy and freedom of expression must be undertaken by the UK Government in order to make a similar programme compatible with data protection and freedom of expression, but using some form of this programme as a plank within Prevent, or working with Sakinah to extend its reach to UK citizens, may increase both effectiveness and appropriateness for the UK.

---

<sup>2155</sup> *ibid.*

<sup>2156</sup> Boucek, C. *The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia* (Combating Terrorism Center, 15 August 2008) <<https://www.ctc.usma.edu/posts/the-sakinah-campaign-and-internet-counter-radicalization-in-saudi-arabia>> accessed November 2016.

<sup>2157</sup> *ibid.*

<sup>2158</sup> bin Khalid al-Saud, A. *The Tranquility Campaign: A Beacon of Light in the Dark World Wide Web, Perspectives on Terrorism* Vol. 11 No. 2 (2017), <<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/596/html>> accessed April 2018.

NB. Abdullah bin Khalid al-Saud is a member of the House of Saud, but holds a PhD and is a Visiting Research Fellow at the International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London and an Assistant Professor, Naif Arab University for Security Sciences (NAUSS), Riyadh, Saudi Arabia.

<sup>2159</sup> *ibid.*

<sup>2160</sup> *ibid.*

#### **7.5.3.1.e. Kingdom of Saudi Arabia: Specific Cybercrime laws**

Here, Saudi Arabia has a gap within the application of its stringent Internet laws. As noted in chapter six,<sup>2161</sup> despite introducing an Anti-Cybercrime Law in 2007, and strengthening penalties on computer misuse, Saudi citizens are still at a heightened risk of cyberlaundering, which is a key concern in the fight against terrorist financing and Internet transactions.<sup>2162</sup> Predicted to grow to \$69 billion by 2020, cyberlaundering in Saudi Arabia is significant; meaning that terrorist financiers can hide their transactions with relative ease. Combined with a lack of a specific offence of using computers as a conduit for committing traditional financial crime, and the vulnerability of Saudi citizens to online fraud, Saudi Arabia must include these into its 2007 law. While it signed the Arab Cybercrime Agreement in 2012,<sup>2163</sup> it has yet to ratify its provisions, and even the Agreement has definitions which are too broad to tackle cybercrime effectively.

As such, even a partial acceptance or adaptation of the European Convention on Cybercrime's articles would assist Saudi Arabia's authorities in capturing fraudulent transactions, as well as those related to online money laundering. As will be elaborated on under 7.5.2.d., this far-reaching Convention includes tackling traditional crimes through use of the computer, which would ultimately capture terrorist financing and money laundering. At the very least, it should incorporate the Arab Cybercrime Agreement which does attempt to tackle online credit card fraud, amongst other cybercrimes.

---

<sup>2161</sup> Chapter six, 6.4.

<sup>2162</sup> *ibid.*

<sup>2163</sup> *ibid.*

#### **7.5.3.2.      Improvements to international law**

Improvements to domestic law can only go so far, as limits to their application include that of jurisdiction and mutual co-operation with other countries. Only true changes to every country's fight against terrorist financing via the Internet can be made through international agreement, as evidenced in the immediate aftermath of 9/11. Four important changes must therefore be made to ensure that every country can set aside resources and both effectively and appropriately combat terrorist financing; two of which are long-term changes and two which can be made in the more immediate future. Primarily, there must be a single definition of terrorism. It is not enough that the United Nations and its members rely on both interpretation spread across a number of Conventions and Resolutions, as well as sovereign views on what determines a terrorist act. This is a long-term solution to a problem which has troubled the UN and its members for many years; doubtless there would have to be international agreement as to what constitutes terrorism, the evaluation of which would be the subject of another thesis in itself. Second, and more immediately, international organisations such as the Financial Action Task Force should re-evaluate the application of the Suspicious Activity Report regime, as it is clearly inappropriate to use in cases of counter-terrorist financing, especially when financial institutions are under a significant legal burden to trace these transactions. Third, another long-term solution is to investigate the ability of the UN or an associated international body, to oversee the way in which domestic jurisdictions govern their citizens' use of the Internet, but this again would have to be subject to international agreement, which would be difficult to foresee in the near future, as it has been of critical international debate for many years. Finally, the suggestion that the UN Security Council submits a resolution for UN Members to adopt the European Cybercrime Convention is something which would be more applicable in

the near future. Cybercrime itself is of national and international concern; it can bring down Governments through cyberattacks and hacking, as well as mask terrorist financing. Consequently, the UN Security Council would have a mandate to intervene in this area as it is a threat to peace and security. Ultimately, this thesis recommends the application of the fourth recommendation - to adopt the European Convention on Cybercrime through a Security Council Resolution - as an international way of balancing the effectiveness of counter-terrorist financing through Internet transactions with the appropriateness of maintaining some privacy elements in accordance with sovereign principles.

#### **7.5.3.2.a. A definition of terrorism**

The lack of a single definition of terrorism exposes difficulties for individual countries to determine the difference between a terrorist website soliciting donations and a humanitarian website which is asking for support, creating concerns about the appropriateness of their counter-terrorism laws. This is evident in Saudi Arabia, whereby intensive Internet filtration systems block,<sup>2164</sup> for example, the websites of internationally recognised humanitarian websites such as Amnesty International.<sup>2165</sup> Furthermore, its definition of terrorism includes references to harming its reputation and status as a country. From a strictly religious society based on Shari'ah law,<sup>2166</sup> with lèse-majesté laws, it is not difficult to see that its website blocks extend further than pornographic or terrorist-related websites, and that it has used counter-terrorism laws to

---

<sup>2164</sup> *ibid.*

<sup>2165</sup> Amnesty International *Amnesty International website 'blocked in Saudi Arabia'* (25 July 2011) <<https://www.amnesty.org/en/latest/news/2011/07/amnesty-international-website-eblocked-saudi-arabia/>> accessed November 2016.

<sup>2166</sup> Chapter three, 3.2.4.

silence its online critics.<sup>2167</sup> Such extreme application is by no means restricted to Saudi Arabia. To a lesser extent, the UK also uses website filtration techniques, also removing certain website pages which are considered extremist.<sup>2168</sup> Yet, while there is narrow definition of terrorism, it is difficult to determine which pages have been removed and thus whether the UK's strategy is appropriate.

Moreover, in relation to communications and data surveillance, the lack of a definition is problematic, as some countries bend or ignore completely the Universal Declaration of Human Rights when dealing with terrorist communications, further eroding the rights of freedom of expression and privacy for the majority of Internet users. As mentioned earlier,<sup>2169</sup> the US and the UK, through the exposure of the PRISM and TEMPORA programmes, had shown how far the CIA and MI5 would take data surveillance under the banner of 'national security', an exception to application of the Universal Declaration. The coverage of these programmes also prompted different reactions – while the US and the EU moved towards further data protection, the UK has sought to protect its mass surveillance techniques.<sup>2170</sup> Merely a few steps away from the UK's proposals in the Investigatory Powers Act is Saudi Arabia, which has very little legal framework to properly protect users of the Internet in the region.<sup>2171</sup> Instead, those who have raised political concerns online are subject to counter-terrorism laws, including closed courts, leading one to conclude that both its definition of terrorism is too broad.<sup>2172</sup> In only very limited circumstances do either the UK or the US have court sessions *in camera*, in accordance with the Universal Declaration. Therefore, Saudi's reaction towards online comment and political opposition,

---

<sup>2167</sup> Chapter six, 6.2.1.

<sup>2168</sup> Chapter five, 5.2.1.

<sup>2169</sup> Chapter seven, 7.5.1; 7.5.2.1.; 7.5.2.2.; 7.5.3.1.c.

<sup>2170</sup> *ibid.*

<sup>2171</sup> Chapter six, 6.2.2.

<sup>2172</sup> *ibid.*

as well as the UK's movements towards a more expansive surveillance regime further bolsters the case for an international definition of terrorism.

**7.5.3.2.b. A re-evaluation of the Suspicious Activity Report system**

Evidently, the Suspicious Activity Report regime outlined by the 1999 Convention has been unable to cope with the demands of globalisation and solving technology. As outlined previously within this chapter,<sup>2173</sup> this is clear by the use of the suspicious transaction reporting systems, whereby the US and the UK have a plethora of reports for law enforcement authorities to sift through,<sup>2174</sup> and the under-reporting by Saudi financial institutions.<sup>2175</sup> This lack of balance calls into question the effectiveness of this system – as it was already in place when the 9/11 terrorists financed their acts through the legitimate financial system in the US and was missed by law enforcement authorities.<sup>2176</sup> To use an anti-money laundering technique for counter-terrorist financing seems to create further difficulties for individual countries to combat; even more so when financial institutions themselves have been involved in covering up vital information relating to terrorist financing. A more uniform application of these reports is therefore needed to ensure that countries neither under- nor over-report, especially with Internet transactions. Furthermore, Customer Due Diligence (CDD) requirements are essential in higher risk, non-face-to-face transactions such as online banking. Yet Saudi Arabia again had huge gaps in the application of this requirement, by the fact that financial institutions did not carry out CDD checks on existing customers when they opened online bank accounts.<sup>2177</sup> The FATF has attempted to address this

---

<sup>2173</sup> Chapter seven, 7.3.2; 7.5.1; 7.5.3.1.a.

<sup>2174</sup> Chapter four, 4.3.2. and chapter five, 5.3.2.

<sup>2175</sup> Chapter six, 6.3.2.

<sup>2176</sup> Chapter four, 4.3.2.

<sup>2177</sup> Chapter six, 6.3.2.



issue by providing its members with guidance, but this is of limited effectiveness as it is soft law. As such, by re-evaluating both the CDD checks and the Suspicious Activity Report programme, as well as providing guidance in this area for banks and financial institutions when dealing with terrorist financing conducted through the Internet, both the UN and the Financial Action Task Force have a role to play in ensuring that Suspicious Activity Reports are used effectively and appropriately.

#### **7.5.2.c. Internet Governance**

Alongside a definition of terrorism and a re-evaluation of the reliance on Suspicious Activity Reports needs to be serious consideration of Internet governance. While attempts have been made before the UN,<sup>2178</sup> these have included social and political points on terrorism, catching those communications which may be anti-establishment, but not necessarily a terrorist threat if one considers the definitions used by the US and the UK. Furthermore, it is clear that the US, UK and EU are in favour of a more disassociated organisation,<sup>2179</sup> free from political control but able to influence policy discussion about the Internet, such as ICANN. Such heated debates are inevitable surrounding Internet governance, as the Internet was formed as a way of communicating without overarching government control, yet with the rise of ISIL and other technologically aware terrorist groups, the current system of combating terrorist financing via online transactions, as well as online communications, simply does not work. Therefore, establishing an independent organisation with principles for user identification, along the lines of ICANN, but which has an agreement with the UN, as the International Telecommunications Union has, may be a compromise. This would

---

<sup>2178</sup> Chapter seven, 7.2.2.

<sup>2179</sup> *ibid.*

enable law enforcement authorities to identify suspected donors and financiers while having an overarching framework to protect freedom of expression and privacy, and would be free from political control. Finally, the UN may also have to re-examine the enforcement of its privacy standards to further protect the majority of Internet users from intrusive, and often unnecessary, surveillance, by intelligence agencies. While the UNHCR resolved in 2012 that Internet users should expect the same rights online as offline,<sup>2180</sup> this is yet to be apparent in, for example, Saudi Arabia, because its Resolutions are non-binding.<sup>2181</sup> By considering these measures, the UN can truly balance effectiveness and appropriateness through creating a uniform international legislative response towards locating online terrorist finances and preventing their use in terrorist acts. However, this is a solution which still seems to elude the UN's General Assembly.

#### **7.5.3.2.d. Adoption of the European Cybercrime Convention 2001 through a Security Council Resolution**

By comparison, another international instrument, the European Council's 2001 Convention on Cybercrime seems to strike a balance between an effective and an appropriate way of tracing and prosecuting perpetrators of terrorist financing who use the Internet to communicate and transfer their funds. Without an international framework of sorts, as Marion notes, "[e]ach country has its own laws regarding cybercrimes and there is no consistency amongst them",<sup>2182</sup> which has been highlighted throughout this

---

<sup>2180</sup> *ibid.*

<sup>2181</sup> *ibid.*

<sup>2182</sup> Marion, N. *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, International Journal of Cyber Criminology (2010) Vol 4 Issue 1&2 700, 701 <<http://www.cybercrimejournal.com/marion2010ijcc.pdf>> accessed April 2018.

thesis. Quite simply, the lack of a joined up international approach towards cyber-crime misses finances generated by terrorists through these means. Countries like Saudi Arabia, despite strong Internet security are inherently vulnerable to cyber-crime<sup>2183</sup> and, to a lesser extent, so are the UK and the US.<sup>2184</sup> The UN should therefore build upon its ventures into Internet governance, by ratifying the Council of Europe's Cybercrime Convention 2001. This would provide some clarity over abusing the Internet for criminal purposes and allow the formulation of an effective global response.

Signed or ratified by nearly 60 countries, including non-members of the Council of Europe,<sup>2185</sup> the Convention itself is split into three main categories: first, criminal offences are outlined,<sup>2186</sup> which include computer-related offences such as fraud,<sup>2187</sup> and content-related offences such as child pornography.<sup>2188</sup> Second, investigatory powers are outlined under s.2, including data retention,<sup>2189</sup> and the interception of data content,<sup>2190</sup> yet these are tempered with safeguards outlined in Article 15, which include that the establishment, implementation and application of powers under domestic law has to provide for the adequate protection of human rights and liberties, focusing on proportionality of investigatory powers.<sup>2191</sup> Third, the Convention provides for international co-operation,<sup>2192</sup> specifically stating that parties should afford *“one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems*

---

<sup>2183</sup> Chapter six, 6.4.

<sup>2184</sup> Chapter four, 4.4.; chapter five 5.4.

<sup>2185</sup> Council of Europe, Chart of signatures and ratifications of Treaty 185, accessed 13 April 2018.

<sup>2186</sup> European Treaty Series No. 185 Convention on Cybercrime (23 November 2001), s.1 Title II.

<sup>2187</sup> *ibid* Article 8.

<sup>2188</sup> *ibid* Article 9.

<sup>2189</sup> *ibid* Article 16.

<sup>2190</sup> *ibid* Article 21.

<sup>2191</sup> *ibid* Article 15.

<sup>2192</sup> *ibid* Chapter III.

*and data, or for the collection of evidence in electronic form of a criminal offence”*.<sup>2193</sup>

Yet, clearly, the difficulty in countries such as Saudi Arabia, is the lack of technological and legal capabilities to deal with what is a unique and constantly evolving criminal area. Consequently, signatories to the 2001 Convention have been afforded technological and legal support, through Council of Europe and the European Union’s joint project between 2013-2016 on ‘Global Action on Cybercrime’<sup>2194</sup> (GLACY), and finally the establishment of the Council of Europe’s Cybercrime Programme Office (C-PROC) to build global capacity to combat cybercrime.<sup>2195</sup> GLACY’s objectives are simple, essentially “*to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime*”,<sup>2196</sup> through harmonising legislation, judicial training, law enforcement capacities and information sharing.<sup>2197</sup> Similarly, C-PROC has been established to help build capacity through: strengthening legislation on cybercrime and electronic evidence (in line with rule of law and human rights),<sup>2198</sup> training judges, prosecutors and law enforcement;<sup>2199</sup> establishing specialised cybercrime and forensic units, as well as improving interagency co-operation;<sup>2200</sup> as well as promoting both public and private co-operation and enhancing effectiveness of international co-operation.<sup>2201</sup> The resulting projects of both include the ‘iPROCEEDS’ project in

---

<sup>2193</sup> *ibid* Article 25(1).

<sup>2194</sup> Council of Europe *Global Action on Cybercrime* <<https://www.coe.int/en/web/cybercrime/glacy>> accessed 13 April 2018.

<sup>2195</sup> Council of Europe *Cybercrime Programme Office* <<https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc->> accessed 13 April 2018.

<sup>2196</sup> Council of Europe *Global Action on Cybercrime* <<https://www.coe.int/en/web/cybercrime/glacy>> accessed 13 April 2018.

<sup>2197</sup> *ibid*.

<sup>2198</sup> Council of Europe *Cybercrime Programme Office* <<https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc->> accessed 13 April 2018.

<sup>2199</sup> *ibid*.

<sup>2200</sup> *ibid*.

<sup>2201</sup> *ibid*.

South-Eastern Europe and Turkey to target proceeds from online crime<sup>2202</sup> and expand the capacity of each participant to search, seize and confiscate cybercrime proceeds as well as money laundering.<sup>2203</sup> Furthermore the Global Action on Cybercrime provides assistance to signatories to the Convention, including Morocco, the Philippines, Senegal, Sri Lanka and South Africa, so that they may be able to share their experiences within their region.<sup>2204</sup> Consequently, by backing up the Convention with capacity-building projects, the Council of Europe is able to oversee effective and appropriate application of its provisions.

While critics such as Marion state the Convention is largely ‘symbolic’,<sup>2205</sup> meaning that countries who have signed it would apply it differently if at all,<sup>2206</sup> adopting this through a Security Council Resolution would also be a more immediate and binding way of combating both cybercrime and the use of the Internet by terrorist financiers. As with the 1999 UN Convention for the Suppression of the Financing of Terrorism and the resulting Security Council 1373, stating that there is a threat to international security and peace through cybercrime would not be a major leap from the threat of terrorism. By also using capacity-building techniques to include Member States through enhancing existing legislation creates further international co-operation - a similar model to that used by the Financial Action Task Force through its peer-to-peer evaluations of members and their AML/CTF procedures - this would enhance the ability of the UN to oversee not only an appropriate and effective way of dealing with both the issue of cybercrime as a whole, but also the use of the Internet by terrorist

---

<sup>2202</sup> Council of Europe *iPROCEEDS – Targeting crime proceeds on the internet in South Eastern Europe and Turkey* <<https://www.coe.int/en/web/cybercrime/iproceeds>> accessed 13 April 2018.

<sup>2203</sup> *ibid.*

<sup>2204</sup> Council of Europe *Global Action on Cybercrime* <<https://www.coe.int/en/web/cybercrime/glacy>> accessed 13 April 2018.

<sup>2205</sup> *ibid* Marion, N, 703.

<sup>2206</sup> *ibid.*

financiers. What is now needed is the impetus to make such a change.

Balancing threat with security is today's key challenge.

## **LIST OF ABBREVIATIONS**

<b>1999 Convention</b>	-	Convention for the Suppression of the Financing of Terrorism 1999
<b>7/7</b>	-	7 July 2005
<b>9/11</b>	-	11 September 2001
<b>ACLU</b>	-	American Civil Liberties Union
<b>AEDPA</b>	-	Antiterrorism and Effective Death Penalty Act of 1996
<b>AML</b>	-	Anti-Money Laundering
<b>ATCSA</b>	-	Anti-terrorism, Crime and Security Act 2001
<b>ATM</b>	-	Automatic Telling Machine
<b>BCCI</b>	-	Bank of Credit and Commerce International
<b>BSA</b>	-	Bank Secrecy Act of 1970
<b>C-PROC</b>	-	Council of Europe Cybercrime Programme Office
<b>CDD</b>	-	Customer Due Diligence
<b>CIA</b>	-	Central Intelligence Agency
<b>CIP</b>	-	Customer Identification Program
<b>CJEU</b>	-	Court of Justice of the European Union
<b>CMA</b>	-	Computer Misuse Act 1990
<b>CITC</b>	-	Communications and Information Technology Commission
<b>CoE</b>	-	Council of Europe
<b>CRS</b>	-	Congressional Research Service
<b>CTF</b>	-	Counter-Terrorist Financing
<b>CTIRU</b>	-	Counter Terrorism Internet Referral Unit
<b>Cybercrime Convention</b>	-	Council of Europe Convention on Cybercrime
<b>DoJ</b>	-	Department of Justice
<b>DRIPA</b>	-	Data Retention and Investigatory Powers Act 2014

<b>ECHR</b>	-	European Convention on Human Rights
<b>ECrthR</b>	-	European Court of Human Rights
<b>ESCWA</b>	-	UN Economic and Social Commission for Western Asia
<b>EU</b>	-	European Union
<b>EUROPOL</b>	-	European Union Agency for Law Enforcement Co-operation
<b>FATF</b>	-	Financial Action Task Force
<b>FBI</b>	-	Federal Bureau of Investigations
<b>FCA</b>	-	Financial Conduct Authority
<b>FinCEN</b>	-	Financial Crimes Enforcement Network
<b>FISA</b>	-	Foreign Intelligence Surveillance Act of 1978, 2008
<b>FISC</b>	-	Foreign Intelligence Surveillance Court
<b>FIU</b>	-	Financial Intelligence Unit
<b>FSA</b>	-	Financial Services Authority
<b>FTATC</b>	-	Foreign Terrorist Asset Tracking Center
<b>G7/G8</b>	-	Group of 7/8
<b>GCHQ</b>	-	Government Communications Headquarters
<b>GLACY</b>	-	Council of Europe Global Action on Cybercrime
<b>HAMAS</b>	-	Harakat al-Muqawamah al-Islamiyyah
<b>HBUS</b>	-	HSBC Bank United States
<b>HBMX</b>	-	HSBC Bank Mexico
<b>HSBC</b>	-	Hong Kong Shanghai Banking Corporation
<b>ICANN</b>	-	Internet Corporation for Assigned Names and Numbers
<b>ICR</b>	-	Internet Connection Records
<b>IEEPA</b>	-	International Emergency Economic Powers Act of 1977
<b>IMF</b>	-	International Monetary Fund



<b>IOCA</b>	-	Interception of Communications Act 1985
<b>IP</b>	-	Internet Protocol
<b>IPT</b>	-	Investigatory Powers Tribunal
<b>ISIL</b>	-	Islamic State of Iraq and the Levant
<b>IRA</b>	-	Irish Republican Army
<b>IRS</b>	-	Internal Revenue Services
<b>ISP</b>	-	Internet Service Provider
<b>ITU</b>	-	International Telecommunications Union
<b>IWF</b>	-	Internet Watch Foundation
<b>KYC</b>	-	Know Your Customer
<b>Lisbon Treaty</b>	-	Treaty of Lisbon Amending the Treaty on the European Union and Treaty Establishing the European Community
<b>MENAFATF</b>	-	Middle East North Africa Financial Action Task Force
<b>MLA</b>	-	Mutual Legal Assistance
<b>MLCA</b>	-	Money Laundering Control Act of 1986
<b>MLR</b>	-	Money Laundering Regulations 2007
<b>MMORPG</b>	-	Massively Multiplayer Online Role Playing Games
<b>MOSA</b>	-	Ministry of Labour and Social Affairs
<b>NAO</b>	-	National Audit Office
<b>NCA</b>	-	National Crime Agency
<b>NGO</b>	-	Non-Governmental Organisation
<b>NHS</b>	-	National Health Service
<b>NSA</b>	-	National Security Agency
<b>NSL</b>	-	National Security Letter
<b>ODI</b>	-	Overseas Development Institute
<b>OECD</b>	-	Organisation for Economic Co-operation and Development
<b>Palermo Convention</b>	-	UN Convention Against Transnational Organised Crime 2001

<b>Resolution 1373</b>	-	UN Security Council Resolution S/RES/1373
<b>RICO</b>	-	Racketeer Influenced and Corrupt Organizations Act of 1970
<b>RIPA</b>	-	Regulation of Investigatory Powers Act 2000
<b>SAAR</b>	-	Shaykh Sulayaman Abd al-Aziz al-Rahji Foundation
<b>SAFIU</b>	-	Saudi Arabia Financial Intelligence Unit
<b>SAMA</b>	-	Saudi Arabian Monetary Authority
<b>SAR</b>	-	Suspicious Activity Report
<b>SNIA</b>	-	Saudi National Intelligence Agency
<b>STR</b>	-	Suspicious Transaction Report
<b>SWIFT</b>	-	Society for Worldwide Interbank Financial Communications
<b>TAFA</b>	-	Terrorist Asset Freezing Act 2010
<b>UK</b>	-	United Kingdom
<b>UN</b>	-	United Nations
<b>UNHRC</b>	-	UN Human Rights Council
<b>UNSC</b>	-	UN Security Council
<b>USA PATRIOT Act</b>	-	Uniting and Strengthening America by Providing Appropriate Tools Required to Obstruct Terrorism Act of 2001
<b>US</b>	-	United States
<b>Vienna Convention</b>	-	UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988
<b>VPN</b>	-	Virtual Private Network
<b>WCIT-12</b>	-	World Conference on International Telecommunications
<b>WSIS</b>	-	World Summit on the Information Society

## **BIBLIOGRAPHY**

### **Table of Cases:**

#### **United States Cases:**

*Schenck v. United States* 249 U.S. 47 (1919)

*Olmstead v. United States* 277 U.S. 438 (1928)

*Freedman v. Maryland* 380 U.S. 51, 58-59 (1965)

*Berger v. New York* 388 U.S. 41 (1967)

*Katz v. United States* 389 U.S. 347 (1967)

*Brandenburg v. Ohio* (1969) 395 U.S. 444

*United States v. U.S. District Court* 407 U.S. 297 (1972)

*California Bankers' Association v. Schultz* 416 U.S. 21 (1974)

*United States v. Miller* 425 U.S. 435, 442 (1976)

*United States v. Thompson* 603 F.2d 1200 (5<sup>th</sup> Cir 1979)

*Chiarella v. United States* (1980) 445 U.S. 222

*United States v. Bank of Nova Scotia* 691 F.2d 1384 (11<sup>th</sup> Circ. 1982) 462 US 1119 (1983)

*In Re. Grand Jury Subpoena: Marc Rich and Co.* A.G. 707 F.2d 663 (2d Cir. 1983)

*United States v. First National Bank of Boston* CR 85 52-MA (D. Mass February 7 1985)

*United States v. Anzalone* 766 F.2d 676 (1<sup>st</sup> Cir 1985)

*United States v. Varbel* 780 F.2d 758 (9<sup>th</sup> Cir 1986)

*United States v. Denmark* 779 F.2d 1559 (11<sup>th</sup> Cir 1986)

*United States v. Boesky* 674 F.Supp. 1128 (1987)

*United States v. Morris* 928 F.2d 504 (2d Cir. 1991)

*United States v. Jurado-Rodriguez* 907 F. Supp. 568 (E.D.N.Y. 1995)

*United States v. Yousef* 925 F. Supp. 1063 (S.D.N.Y.) (1996)

*United States v. Charbonneau* 979 F.Supp 1177 (S.D. Ohio 1997)

*United States v. O'Hagan* 521 U.S. 642, 655 (1997)

*Reno v. American Civil Liberties Union* 521 U.S. 844 (1997)

*United States of America v. Ramzi Ahmed Yousef and Eyud Ismoil*, S1293CR.180 (KTD), October 22,1997, 4734-4735

*Humanitarian Law Project v. Reno* (1998) 9 F. Supp. 2d 1176 (C.D. Cal.)

*Attorney General v. X* 17/09/1419AH (4 January 1999)

*Humanitarian Law Project v. Reno*, 205 F.3d 1130 (9th Cir.(Cal.) Mar. 3, 2000) (No. 98-56062, 98-56280)

*United States v. Cohen* 260 F.3d 68, 68 (2d Cir. 2001)

*Yahoo! Inc. v. La Ligue le Racisme et L'Antisemitisme* 145 F. Supp. 2d 1168 (N.D. Cal. 2001)

*In re. MasterCard Int'l Inc.*, 313 F.3d 257, 262–63 (5th Cir. 2002)

*United States v. Arnout* 02-CR-892 (N,D, III, 1 November 2002)

*United States v. Al-Hussayen* No 03-040 (D. Idaho 2003)

*United States v. Yousef* 327 F. 3d 56 (2<sup>nd</sup> Cir 2003)

*Humanitarian Law Project v. U.S. Dept. of Justice* 352 F.3d 382 (9th Cir.(Cal.) Dec. 3, 2003) (No. 02-55082, 02-55083)

*Humanitarian Law Project v. Ashcroft* 309 F. Supp. 2d 1185, 1192 (CD Cal. 2004)

*Humanitarian Law Project v. Ashcroft* 393 F.3d 902 (2004)

*Ashcroft v. American Civil Liberties Union* (03-218) 542 U.S. 656 (2004) 322 F.3d 240

*Doe v. Ashcroft* 334 F. Supp. 2d 471 (S.D.N.Y. 2004)

*FTC v. Hill* (F.D. Tex. 2004) (No. H 035537)

*United States v. Al-Hussayen* CR03-048-C-EJL (D. Idaho 4 March 2004)

*Humanitarian Law Project v. Gonzales* No. 04-55871 (9th Cir. Apr. 1, 2005)

*American Civil Liberties Union v. Gonzales* 04 Cir. 2614 Vm 6 September 2007

*American Civil Liberties Union v. Gonzalez* (2007) Civ. NO. 98-5591

*United States v. Ahmad* 3:04CR301(MRK)

*Ahmad v. United States* [2006] EWHC 2927 (Admin), [2007] H.R.L.R. 8 30 November 2006

*American Civil Liberties Union et al. v. Mukasey* (3<sup>rd</sup> Cir. 22 July 2008)

*Mukasey v. American Civil Liberties Union et al.* 555 U.S. 1137 (2009)

*United States v. Mahamud Said Omar* 09-CR-242 (2009)

*United States v. Ahmed Ali Omar, Khalid Mohamud Abshir, Zakaria Maruf, Mohamed Abdullahi Hassan and Mustafa Ali Salat* 09-CR-50 (2009)

*United States v. Kamal Hassan* 09-CR-38 (2009)

*United States v. Abdifatah Yusuf Isse* 09-CR-50 (2009)

*United States v. Salah Osman Ahmed* 09-CR-50 (2009)

*United States v. Kassir* 04 Cr. 356 (JFK), 2009 WL 910767, at \*4 (S.D.N.Y. 2<sup>nd</sup> April, 2009)

*KindHearts for Charitable Humanitarian Development Inc v. Timothy Geithner et al.* Case 3:08c v 02400 (18 August 2009)

*Thomas Dart, Sheriff of Cook County v. Craigslist Inc.* 665 F. Supp. 2d 961 (N.D. Ill. Oct. 20, 2009)

*United States v. Under Seal* 06-2125 4<sup>th</sup> Circuit Court of Appeals; *In Re: Grand Jury Subpoena* (24 February 2010)

*Doe v. Holder* S.D.N.Y. 04 Civ. 2614 (VM) (direct) (2010)

*Holder v. Humanitarian Law Project et al* 130 S. Ct. 2705 (2010)

*United States v. Zacarias Moussaoui* 591 F.3d 263 (4th Cir. 2010)

*United States v. Colleen LaRose* E.D. Pa 1 February 2011

*United States v. Jamie Paulin Ramirez* Eastern District of Pennsylvania 8 March 2011

*Amnesty International USA et al. v. James R. Clapper Jr et al.* 638 F.3d 118 (2d Cir. 2011)

*United States v. Mohammed el-Mezain, Ghassan Elashi, Shukri Abu Baker, Mufid Abdulqader, Abdulrahman Odeh, Holy Land Foundation for Relief and Development* No. 09-10560 F.3d 2011 WL 6058592 (5th Cir. Dec. 7, 2011)

*United States v. Mustafa (Kassir)* (2. Cir 2011)

*United States v. Mehanna* No. 09-cr-10017-GAO (D. Mass. 2011)

*Jewel v. NSA* 673. F. 3d 902 (Ct.App, 9<sup>th</sup> Cir. 2011); No C 08-cv-4373 VRW, MDL No C 06-1791 VRW, No C 07-0693 VRW (Dist.Ct. N.D. CA January 10 2010)

*Center for Constitutional Rights v. Obama* 3:07-cv-01115-VRW (N.D. Cal. ) (2011)

*United States v. El Mezain et al.* No. 09-10560 F.3d 2011 WL 6058592 (5th Cir. Dec. 7, 2011), 7; 11

US Grand Jury Sealed Indictment *United States v. Liberty Reserve S.A. Arthur Budovsky, Vladimir Katz, Ahmed Yassine Abdelghani, Allan Esteban Hidalgo Jiminez, Azzeddine El Amine, Mark Marmilev and Maxim Chukharev* (2013) S.D.N.Y. 13 Crim 368

*United States v. Mehanna* 735 F.3d 32 (1st Cir. 2013)

*Clapper v. Amnesty International USA et al* 638 F. 3d 118 (26 February 2013)

*United States v. Dzhokhar A. Tsarnaev* (District Court of Massachusetts, Case Number: 1:13-cr-10200)

*Klayman et al. v. Obama* Memorandum and Opinion (16 December 2013) Civ. Action No. 13-0851

*John Patrick O'Neill et al. v. Al Rajhi Bank et al.* [2014] United States Supreme Court No. 13-318

*United States of America v. Ross William Ulbricht a/k/a 'Dread Pirate Roberts', a/k/a 'DPR', a/k/a 'Silk Road'* 14-cr-68 (October 30, 2014)

*United States v. Ali Shukri Amin* Criminal No: 1:15-cr-164 in the Eastern District of Virginia, Alexandria Division (2015)

### **United Kingdom Cases:**

*R v Cuthbertson* [1981] 1 AC 470

*R v Gold and Shifreen* (1987) 3 All ER 618; (1987) 3 WLR 803 (C/A); (1988) 2 All ER 186; [1988] A.C. 1063

*DPP v Bignall* [1998] 1 Cr. App. R. 1; (1997) 161 J.P. 541; [1997-98] Info. T.L.R. 168; [1998] I.T.C.L.R. 33; [1998] Masons C.L.R. Rep. 141; [1998] Crim. L.R. 53; (1997)

*R v Bow Street Metropolitan Stipendiary Magistrate and Another, ex parte Government of the United States of America* [2000] 2 AC 216 [1999] 3 W.L.R. 620; [1999] 4 All E.R. 1; [2000] 1 Cr. App. R. 61

*R v P* (2001) 2 All ER 58

*R (on the application of ntl Group Ltd) v Ipswich Crown Court* 22 July 2002 [2002] EWHC 1585 (Admin), [2003] Q.B. 131

*Mahfouz v Brisard & others* [2004] EQHC 1735 (QB)

*bin Mahfouz v Jean Charles Brisard* [2006] EWHC 1191 (QB)

*Al-Amoudi v Brisard* [2007] 1 WLR 113

*R v Tsouli, Mughal and Al-Daour* [2007] EWCA Crim 3300

*R v K* [2008] 2 WLR 1026, [2008] EWCA Crim 185

*Attorney General's Reference Nos 85 86 and 87 of 2007 (Youlis Tsouni and others)* [2007] EWCA Crim 3300; [2008] Cr. App. R. (S.) 45

*A v Her Majesty's Treasury* [2008] 2 C.M.L.R. 44

*R v Malik* [2008] All ER (D) 201 (Jun)

*R v Waheed Ali* [2009] EWCA Crim 2396

*A v HM Treasury* [2010] UKSC 2; [2010] 2 W.L.R. 378

*HM Treasury v Ahmed and others* [2010] UKSC 2

*HM Treasury v Mohammed Jabar Ahmed and others; Her Majesty's Treasury v Mohammed al-Ghabra; R (on the application of Hani El Sayed Sabaei Youssef) v Her Majesty's Treasury* [2010] UKSC 2

*R v Terence Roy Brown* [2011] EWCA Crim 2751 [2012] Cr App R (S.) 10

*R v Ahmad (Bilal Zaheer)* [2012] EWCA Crim 959 [2013] 1 Cr. App. R. (S.) 17

*R. v. Nasser et al. (Irfan Nasser)* [2012] EWCA Crim. 2

*R (on the application of HS2 Action Alliance Limited) (Appellant) v The Secretary of State for Transport and another (Respondents)*, [2014] UKSC 3

*R v Adebolajo and another* [2014] All ER (D) 37

*Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others* Case Nos IPT/13/77/CH, 13/92/CH, 13/194/C and 13/204/CH [2015] UKIPTrib 13\_77-H, judgements of 5 December 2014 and 6 February 2015.

*R (on the application of David Davis MP, Tom Watson MP, Peter Brice, Geoffrey Lewis) v The Secretary of State for the Home Department and Open Rights Group, Privacy International, The Law Society of England and Wales* [2015] EWHC 2092 (Admin)

*R v Forhad Rahman, Kristen Brekke and Adeel Ulhaq* (February 2016) (Crown Prosecution Service *R v Forhad Rahman, Adeel Brekke and Kaleem Kristen Ulhaq* <<https://www.cps.gov.uk/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-end-2006>> accessed November 2016)

### **European Union Cases:**

C-101/01 *Bodil Lindqvist v Åklagarkammaren i Jönköping* [2003] ECR I-12971

C-402/05 P and C-415/05 P *Kadi v Council of the European Union and Commission of the European Communities* (2008)

Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd. (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General and Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others; Digital Rights Ireland Ltd v Minister of Communications & Ors.* [2010] IEHC 221

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (24 November 2011)

Cases C-411/10 and C-493/10, *N.S. v Home Secretary and M.E. v. Refugee Applications Commissioner* [2011] EUECJ C-411/10 (21 December 2011)

Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (16 February 2012)

C-617/10 *Åklagaren v Hans Åkerberg Fransson* (26 February 2013)

Case C-698/15 *Home Secretary v Tom Watson, Peter Brice, Geoffrey Lewis – Intervening Parties: Open Rights Group, Privacy International, The Law Society of England and Wales* (19 July 2016)

C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15)* (19 July 2016)

### **European Court of Human Rights Cases:**



*Handyside v UK* (Application no. 5493/72) Ser A vol.24, (1976) 1 EHRR 737

*Klass and others v The Federal Republic of Germany* (Application no. 5029/71) (1979) 2 EHRR 214, [1978] ECHR 4

*Malone v UK* (1984) 7 EHRR 14, [1984] ECHR 10, [1985] ECHR 5

*Halford v UK* [1997] ECHR 32

*Natunen v Finland* (Application no. 21022/04) (2009) 49 EHRR 810

*Kennedy v United Kingdom* (2010) (Application No. 26839/05)

*Babar Ahmad and Others v The United Kingdom* (Application nos. 24027/07, 11949/08 and 36742/08) [2012] ECHR 609

*In Vejdeland and others v Sweden* (Application no. 1813/07) [2012] ECHR 242

*Yildirim v Turkey* (Application no. 3111/10) HEJUD [2012] ECHR 2074

*Al-Dulimi and Montana Management Inc. v Switzerland* (Application no. 5809/08) (Court (First Instance)), (26 November 2013)

(1) *Big Brother Watch* (2) *Open Rights Group* (3) *English PEN* (4) *Dr Constanze Kurz v United Kingdom* (Application No. 58170/13) [2014] ECHR 93

*Roman Zakharov v Russia* (Application no. 47143/06) (Court (Grand Chamber)), [2015] ECHR 1065

*Szabó and Vissy v Hungary* (Application no. 37138/14) (Court (Fourth Section)), [2016] ECHR 579

*Al-Dulimi and Montana Management Inc. v Switzerland* (Application no. 5809/08) (Court (Grand Chamber)), [2016] ECHR 576

### **Kingdom of Saudi Arabia Cases:**

*Linde et al. v. Arab Bank PLC* (2004) 04 CV 02799 (E.D.N.Y. filed 2 July 2004) (Discovery Order sought before trial - 384 F. Supp. 2d 571 (E.D.N.Y. 2005) and granted - 2006 WL 3422227 (E.D.N.Y. 25 November 2006)

*Almog v. Arab Bank PLC* 471 F. Supp. 2d 257, 285 (E.D.N.Y. 2007)

### **Table of Legislation:**

## **Table of Legislation: United States**

Constitution of the United States 1787 (date effective, 21 June 1788)

Trading with the Enemy Act of 1917 (40 Stat. 411) (12 U.S.C. 95a and 50 U.S.C. App. 1 et seq.)

Federal Trade Commission Act of 1914 (Chapter 311, 38 Stat. 717) (15 U.S.C. 41 et seq.)

Securities Act of 1933 (Title I of Pub. L. 73-22, 48 Stat. 74) (15 U.S.C. 77a et seq.)

Securities Exchange Act of 1934 (Pub.L. 73–291, 48 Stat. 881) (15 U.S.C. 78a et seq.)

Communications Act of 1934 (Pub. L. 73-416, 48 Stat. 1064) (47 U.S.C. 151 et seq.)

United Nations Participation Act of 1945 (Pub. L. 79-264, 59 Stat. 619) (22 U.S.C. 287c et seq.)

Immigration and Nationality Act of 1952 (Pub.L. 82–414, 66 Stat. 163) (8 U.S.C. Ch. 12)

Federal Wire Act of 1961 (Pub. L. 87-216, 75 Stat. 491) (18 U.S.C. Part I Chapter 50)

Interstate and Foreign Travel or Aid in Racketeering Enterprises Act of 1961 (“Travel Act”) (Pub. L. 87–228, 75 Stat. 498) (18 U.S.C. 1952 et seq.)

Truth in Lending Act of 1968 (Pub. L. 90-321 82 Stat. 146) (15 U.S.C. Ch. 41 1601 et seq.)

Title III Omnibus Crime Control and Safe Streets Act of 1968 (Pub.L. 90–351, 82 Stat. 197) (34 U.S.C. 10101 et seq.)

Organized Crime Control Act of 1970 (Pub.L. 91–452, 84 Stat. 922) (18 U.S.C. Ch. 73, 79, 95, 96, 216, 223, 601)

The Racketeer Influenced and Corrupt Organizations Act of 1970 (“RICO”) (Pub. L. 91-452, 84 Stat. 941) (18 U.S.C. 1961 et seq.)

The Financial Recordkeeping and Currency and Transactions Reporting Act of 1970 (“Bank Secrecy Act”) (Pub. L. 91-508, 84 Stat. 1118) (31 U.S.C. 5311 et seq.)

Comprehensive Drug Abuse Prevention and Control Act of 1970 (Pub.L. 91–513, 84 Stat. 1236) (21 U.S.C. Ch. 13, 801 et seq.)

Illegal Gambling Business Act of 1970 (Pub. L. 91–452, title VIII) (18 U.S.C. 1955 et seq.)

Privacy Act of 1974 (Pub.L. 93–579, 88 Stat. 1896) (5 U.S.C. 522 et seq.)

National Emergencies Act of 1976 (Pub.L. 94–412, 90 Stat. 1255) (50 U.S.C. 1601 et seq.)

International Emergency Economic Powers Act of 1977 (Title II of Pub.L. 95–223, 91 Stat. 1626) (50 U.S.C. Ch. 35)

Foreign Intelligence Surveillance Act of 1978 (Pub.L. 95–511, 92 Stat. 1783) (50 U.S.C. Ch. 36)

The Right to Financial Privacy Act of 1978 (Pub. L. 95-630, 92 Stat. 3461) (12 U.S.C. 35)

False Identification Crime Control Act of 1982 (Pub L. No. 97-398, 96 Stat. 2009) (18 U.S.C 1028, 1738)

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (Pub. L. 98-473, 98 Stat. 2190) 18 U.S.C. 1030

Money Laundering Control Act of 1986 (Pub. L. 99-570, 100 Stat. 3207) (18 U.S.C. Ch. 95)

Computer Fraud and Abuse Act of 1986 (Pub. L. 99-174) (18 U.S.C. § 1030)

Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, 100 Stat. 1848) (18 U.S.C. 2701 et seq.)

Internal Revenue Code of 1986 (Pub. L. 99–514, 100 Stat. 2095) (26 U.S.C.)

Anti-Drug Abuse Act of 1988 (Pub. L. 100-690, 102 Stat. 4355) (31 U.S.C. 53)

Annunzio-Wylie Anti-Money Laundering Act of 1992 (under Title XV of the Housing & Community Development Act 1992) (Pub. L. 102-358, 106 Stat. 3672)

Money Laundering Suppression Act of 1994 (under Title IV of the Riegle-Neal Community Development and Regulatory Act 1994) (Pub. L. 103-325 Title IV, 108 Stat. 2243) (31 U.S.C. 5301)

Violent Crime Control and Law Enforcement Act of 1994 (Pub. L. 103-322, 108 Stat. 1796) (42 U.S.C. Ch. 136)

Communications Assistance for Law Enforcement Authorities Act of 1994 (Pub. L. No. 103-414, 108 Stat. 4279) (47 USC 1001)

Executive Order 12,947 *Prohibiting Transactions with Terrorists who threaten to disrupt the Middle East Peace Process* (President William J. Clinton, 1995)

Iran Libya Sanctions Act of 1996 (Pub. L. 104-172 110 Stat. 1541) (50 U.S.C. Ch. 35, 1701 et seq.)

Communications Decency Act of 1996 (Pub. L. 104-104, 110 Stat. 133) (47 U.S.C. 230)

Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) (Pub L. 104-132, 110 Stat. 1214)

Executive Order 13,099 *Prohibiting Transactions with Terrorists who threaten to disrupt the Middle East Peace Process* (President William J. Clinton, 1998)

Protection of Children from Predators Act of 1998 (Pub. L. 105-314, 112 Stat 2974) (18 U.S.C. 1111 et seq.)

Child Online Protection Act of 1998 (Pub. L. 105-277, 112 Stat 2681-728) (15 U.S.C. 6501 et seq.)

Money Laundering and Financial Crimes Strategy Act of 1998 (Pub. L. 105-310, 112 Stat. 2941) (18 U.S.C. Ch. 46)

Executive Order 13,129 *Blocking property and prohibiting transactions with the Taliban* (President William J. Clinton, 1999)

Gramm-Leach Bliley Act of 1999 (Pub.L. 106-102, 113 Stat. 1338) (12 U.S.C.)

Children's Internet Protection Act of 2000 (Pub.L. 106-554, 114 Stat. 2763) (47 U.S.C. 254 et seq.)

Executive Order 13,224 *Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism* (President George W. Bush, 2001)

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (Pub. L. 107-56, 115 Stat. 272)

Homeland Security Act of 2002 (Pub. L. 107-296, 116 Stat. 2135) (6 U.S.C. Ch. 1, 101 et seq.)

Cyber Security Enhancement Act of 2002 H.R. 3428 107<sup>th</sup> Congress

USA PATRIOT Act Improvement and Reauthorization Act of 2005 (Pub. L. 109-177, 120 Stat. 192)

The Unlawful Internet Gambling Enforcement Act of 2006 (Pub. L. 109-347, 120 Stat. 1884) (31 U.S.C. Ch. 53 Subch. IV)

Identity Theft Enforcement and Restitution Act of 2007 (Pub. L. 110-326, Title II, 122 Stat. 3560) (18 U.S.C. 1)

Protect America Act of 2007 (Pub.L. 110-55, 121 Stat. 552) (50 U.S.C. Ch. 36 1801 et seq.)

Foreign Intelligence Surveillance Act of 1978 Amendments Act 2008 (Pub. L. 110-261, 122 Stat. 2436) (50 U.S.C. Ch 36 1801 et seq.)

Financial Recordkeeping and Reporting of Currency and Foreign Transactions (2010) (Title 31 Code of Federal Regulations B Ch. I Part 103/ Title 31 Chapter X CFR §1020.220)

An Act To extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011 (2010) (Pub.L. 111-114)

The PATRIOT Sunsets Extension Act of 2011 (Pub. L. 112-114, 125 Stat. 216) (50 U.S.C. 1801)

Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (“USA Freedom Act”) (Pub. L. 114-23, 120 Stat 200) (50 U.S.C. 1801)

Countering Violent Extremism Act (H.R.2899 — 114th Congress (2015-2016))

### **Table of Legislation: United Kingdom**

Telegraph Act 1863 c. 112 (Regnal. 26 and 27 Vict)

Telegraph Act 1868 c. 110 (Regnal. 31 and 32 Vict)

United Nations Act 1946 c. 45 (Regnal 9 and 10 Geo 6)

Theft Act 1968 c.60

Misuse of Drugs Act 1971 c.38

Northern Ireland (Emergency Provisions) Act 1973 c.53

Prevention of Terrorism (Temporary Provisions) Act 1974 c.56

Prevention of Terrorism (Temporary Provisions) Act 1976 (Continuance Order) 1978 SI 1978/487

Protection of Children Act 1978 c.37

Interception of Communications Act 1985 c.56

Drug Trafficking Offences Act 1986 c.32

Criminal Justice Act 1988 c. 33

Prevention of Terrorism (Temporary Provisions) Act 1989 c.4

Computer Misuse Act 1990 c.18

Northern Ireland (Emergency Provisions) Act 1991 c.24

Money Laundering Regulations 1993 SI 1993/1933

Criminal Justice Act 1993 c.36

Intelligence Services Act 1994 c.13

Criminal Justice and Public Order Act 1994 c.33

Human Rights Act 1998 c.42

Data Protection Act 1998 c.29

Criminal Justice (Terrorism and Conspiracy) Act 1998 c.40

Telecommunications (Data Protection and Privacy) Regulations 1999, SI 1999/2003

Financial Services and Markets Act 2000 c.8

Terrorism Act 2000 c.11

Regulation of Investigatory Powers Act 2000 c.23 ('RIPA')

Anti-terrorism, Crime and Security Act 2001 c.24

Proceeds of Crime Act 2002 c.29

Sexual Offences Act 2003 c.42

Communications Act 2003 c.21

Money Laundering Regulations 2003 SI 2003/3075

Gambling Act 2005 c.19

Prevention of Terrorism Act 2005 c.2

Charities Act 2006 c.50

Police and Justice Act 2006 c.48

Terrorism Act 2006 c.11

Fraud Act 2006 c.35

Terrorism (United Nations Measures) Order 2006 SI 2006/2657

Money Laundering Regulations 2007 SI 2007/2157

Counter Terrorism Act 2008 c.28

Criminal Justice and Immigration Act 2008 c.4

Data Retention (EC Directive) Regulations 2009 SI 2009/859

Terrorist Asset-Freezing (Temporary Provisions) Act 2010 c.2

Terrorist Asset-Freezing etc. Act 2010 c.38

The Regulation of Investigatory Powers (Monetary Penalty Notices and Consents for Interception) Regulations 2011 SI 2011/1340

Charities Act 2011 c.25

Crime and Courts Act 2013 c.22

Data Retention and Investigatory Powers Act 2014 c.27

The Criminal Justice and Data Protection (Protocol 36) Regulations 2014 SI 2014/3141

Counter-Terrorism and Security Act 2015 c.6

Investigatory Powers Act 2016 c.25

### **Table of Legislation: European Union**

Treaty establishing the European Economic Community (Treaty of Rome) 25 March 1957

Council Directive 91/308/EEC *on the prevention of the use of the financial system for the purpose of money laundering* ('First Money Laundering Directive')

Treaty on the European Union (Maastricht Treaty) 7 February 1992

Directive 95/46/EC (24 October 1995) *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

Directive 97/66/EC (15 December 1997) *concerning the processing of personal data and the protection of privacy in the telecommunications sector*

Directive 2000/31/EC (8 June 2000) *Article 45 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market* ('Directive on electronic commerce')

Charter of Fundamental Rights of the European Union 2000/C 364/01

Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union 2000/C 197/01

European Union Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union ('MLAC') & Protocol - Implementation - Extended to Norway and Iceland 2000/C 197/01

Directive 2001/97/EC (4 December 2001) *amending Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering* ('Second Money Laundering Directive')

Directive 2002/58/EC (12 July 2002) *concerning the processing of personal data and the protection of privacy in the electronic communications sector* (Directive on privacy and electronic communications)

Directive 2005/60/EC (26 October 2005) *on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* ("Third Money Laundering Directive")

Directive 2006/24/EC (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*

Directive 2009/136/EC (25 November 2009) *amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*

The Treaty on European Union and the Treaty on the Functioning of the European Union ('Lisbon Treaty'), 13 December 2007

11222/1/2010/REV 1 and COR 1 – C7-0158/2010 – 2010/0178(NLE) *Legislative resolution of 8 July 2010 on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*

Directive 2011/92/EU (13 December 2011) *on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA*

Directive 2014/42/EU (3 April 2014) *on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union*



Directive 2015/849/EU (20 May 2015) *on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC ('Fourth Money Laundering Directive')*

Directive 2016/680/EU (27 April 2016) *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*

### **Table of Legislation: Council of Europe**

Convention for the Protection of Human Rights and Fundamental Freedoms 1950

European Treaty Series No. 141 *Convention on Laundering, Search, Seizure and Confiscation from Proceeds of Crime* (8 November 1990)

European Treaty Series No. 185 *Convention on Cybercrime* (23 November 2001)

European Treaty Series No. 190 *Council of Europe Protocol Amending the European Convention on the Suppression of Terrorism* (15 May 2003)

European Treaty Series No. 198 *Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime and on the Financing of Terrorism* (16 May 2005)

Council of Europe Recommendation R (89) 9 of the Committee of Ministers to Member States on *Computer-Related Crime*

Council of Europe Recommendation (95) 13 *Concerning problems of criminal procedural law connected with information technology* (11 September 1995)

### **Table of Legislation: Kingdom of Saudi Arabia**

Basic Law of Governance (Constitution of Saudi Arabia), Royal Decree No. A/90 dated 27/08/1412H (March 1, 1992) (revised 2005)

Saudi Internet Rules, Council of Ministers Resolution, 12 February 2001 <<http://al-bab.com/saudi-internet-rules-2001>> accessed April 2018

Telecom Act 2001 Issued under the Council of Ministers Resolution No. (74) dated 05/03/1422H (corresponding to 27/05/2001)

Saudi Arabian Monetary Authority *Guidelines to Internet Banking May 2001* (replaced by e-Banking Rules 2010)

Anti Money Laundering Law 2003 Royal Decree No. M/39 25 Jumada II 1424 / 23 August 2003

Saudi Arabian Monetary Authority *Rules Governing the Opening of Bank Accounts* (2003; fourth update 2012) <[http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules\\_Governing\\_the\\_Opening\\_of\\_Bank\\_Accounts\\_ver4.pdf](http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules_Governing_the_Opening_of_Bank_Accounts_ver4.pdf)> accessed June 2018

Saudi Arabian Non-Governmental Commission for Relief and Charity Work Abroad, Royal Decree No.2/1 dated 6/1/1425 AH (February 2004)

Council of Ministers Resolution No. 229 dated 13.08.1425 H (2004) on the transfer of Internet Filtering services to the Communications and Information Technology Commission

Anti Cyber Crime Law 2007 Royal Decree No. M/17 26 March 2007

Electronic Transactions Law 2007 Royal Decree No. M/8 8 Rabi' I- 1428H – 26 March 2007

Saudi Arabian Monetary Authority *e-Banking Rules 2010* <[www.sama.gov.sa/en-US/Laws/BankingRules/E\\_banking\\_Rules.docx](http://www.sama.gov.sa/en-US/Laws/BankingRules/E_banking_Rules.docx)> accessed April 2018

Implementation of the Convention for the Suppression of the Financing of Terrorism Royal Order No. (1804) dated 7, Muharram 1433 A.H. (3 Dec. 2011)

Ministerial Decision No. (1697) dated 20, Rabi' Al-Thani 1433 A.H. (14 March 2012) approving the procedures for implementing the International Convention for the Suppression of the Financing of Terrorism

Penal Law for Crimes of Terrorism and its Financing 2013 Royal Decree No. M/16 of 27 December 2013

## **Table of Legislation: United Nations**

### General Assembly Resolutions:

United Nations Charter 1945

Universal Declaration of Human Rights 1948 (General Assembly Resolution 217A)

UN Treaty Series 1973 Convention for the Suppression of Unlawful Seizure of Aircraft (16 December 1970)

974 UN Treaty Series 1977 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (23 September 1971)

A/RES/3166 (XVIII) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents (14 December 1973)

A/RES/34/146 International Convention against the Taking of Hostages (17 December 1979)

INFCIRC/274 Convention on the Physical Protection of Nuclear Material (3 March 1980)

474 UN Treaty Series 1990 No. 14118 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (24 February 1988)

1678 UN Treaty Series 1992 No.29004 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention) (10 March 1988)

1678 UN Treaty Series 1992 No.29004 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (SUA PROT) (10 March 1988)

UN Treaty Series vol. 1582 No. 27627 Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 ('Vienna Convention')

A/RES/45/121 Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (14 December 1990)

A/RES/49/60 Measures to eliminate international terrorism (9 December 1994)

A/RES/51/210 Measures to eliminate international terrorism (17 December 1996)

A/RES/52/91 Preparations for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (12 December 1997)

A/RES/52/164 International Convention for the Suppression of Terrorist Bombings (UN General Assembly) (15 December 1997)

A/RES/52/165 Measures to eliminate international terrorism (15 December 1997)

A/RES/53/112 Model Treaty on Mutual Assistance in Criminal Matters was adopted by the General Assembly (December 1998)

A/RES/53/110 Preparations for the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (9 December 1998)

A/RES/53/108 Measures to eliminate international terrorism (26 January 1999)

A/RES/54/109 International Convention for the Suppression of the Financing of Terrorism 1999 (9 December 1999)

A/RES/55/25 UN Convention against Transnational Organised Crime (15 November 2000) ('Palermo Convention')

A/RES/55/63 Combating the criminal misuse of information technologies (4 December 2000)

A/RES/56/121 Combating the criminal misuse of information technologies (19 December 2001)

A/RES/57/239 Creation of a global culture of cybersecurity (31 January 2003)

A/RES/58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures (30 January 2004)

A/RES/60/288 The United Nations Global Counter-Terrorism Strategy (8 September 2006)

A/RES/68/167 The right to privacy in the digital age (21 January 2014)

A/RES/69/166 The right to privacy in the digital age (10 February 2015)

#### Security Council Resolutions

S/RES/1267 (1999) on Afghanistan

S/RES/1269 (1999) Responsibility of the Security Council in the maintenance of international peace and security

S/RES/1333 (2000) on the situation in Afghanistan

S/RES/1368 (2001) Counter-Terrorism Implementation Task Force

S/RES/1373 (2001) Threats to international peace and security caused by terrorist acts

S/RES/1566 (2004) Creation of working group to consider measures against individuals, groups and entities other than Al-Qaida/Taliban

S/RES/1617 (2005) Threats to international peace and security caused by terrorist acts

S/RES/2249 (2015) Threats to international peace and security caused by terrorist acts

S/RES/2253 (2015) Threats to international peace and security caused by terrorist acts

#### UN Human Rights Council Resolutions:

A/HRC/RES/12/16 on the Promotion and Protection of all human rights, civil political, economic, social and cultural rights, including the right to development (2 October 2009)

A/HRC/RES/15/21 The rights to freedom of peaceful assembly and of association (10 June 2010)

A/HRC/20/L.13 The promotion, protection and enjoyment of human rights on the Internet (29 June 2012)

A/HRC/26/L.24 The promotion, protection and enjoyment of human rights on the Internet (26 June 2014)

A/HRC/RES/28/16 The right to privacy in the digital age (1 April 2015)

A/HRC/32/L.20 The promotion, protection and enjoyment of human rights on the Internet (27 June 2016)

### **Table of Legislation: Voluntary International Regulations**

Basel Committee Banking Regulations and Supervisory Practices Statement of Principles 1988

Financial Action Task Force 40 Recommendations (1990)

Financial Action Task Force IX Recommendations (2001)

Financial Action Task Force Recommendations (2012) <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed November 2016

Arab Cybercrime Agreement (no. 126 of 2012)

Financial Action Task Force International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (February 2012)

International Monetary Fund Articles of Agreement 1944 (amended effective 1969, 1978, 1992, 2009)  
<<http://www.imf.org/external/pubs/ft/aa/aa04.htm>> accessed November 2016

Wolfsberg Principles <<https://www.wolfsberg-principles.com/publications/wolfsberg-standards>> accessed April 2018

### **Bibliography:**

*9-11 Commission Report* (22 July 2004) <<https://www.9-11commission.gov/report/911Report.pdf>> accessed November 2016

*The International Emergency Economic Powers Act: A Congressional Attempt to control Presidential Emergency Power* (1983) 96 Harvard Law Review 1102

*American Civil Liberties Union wins PATRIOT Act dispute on disclosure of national security letters – ACLU v Gonzales* (04 Cir, 2614 Vm) 6<sup>th</sup> September 2007 Computer Law and Security Report 2007 23(6) 490-491

*Access Now Written Evidence to the Public Bills Committee* IPB 72 (April 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB72.htm)> accessed November 2016

Acharya, A. *Small amounts for big bangs? Rethinking responses to “low cost” terrorism* (2009) 12(3) Journal of Money Laundering Control 285

Adams, J. *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet* (1996) 12 Santa Clara Computer and High Tech Law Journal 403

Addicott, J.F. & McCaul, M.T. *The Protect America Act of 2007: A framework for improving intelligence collection in the war on terror* (2008-9) 13 Tex. Rev. L & Policy 43

Akdeniz, Y., Taylor, N. & Walker, C. *Regulation of Investigatory Powers Act 2000: Part 1: Bigbrother.gov.uk: State surveillance in the age of information and rights* (2001) Criminal Law Report Feb, 73

Akdeniz, Y. *To block or not to block: European approaches to content regulation, and implications for freedom of expression* (2010) 26 Computer Law & Security Review 260

Akindemowo, O.E. *The pervasive influence of anti-terrorist financing policy: post 9/11 non bank electronic money issuance* (2004) 19(8) *Journal of International Banking Law and Regulation* 289

Alanezi, F. & Brooks, L. *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT)* Twentieth Americas Conference on Information Systems (Savannah, 2014) <[aisel.aisnet.org/cgi/viewcontent.cgi?article=1156&context=amcis2014](http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1156&context=amcis2014)> accessed November 2016

Aldrich, R.W. *Cyberterrorism and Computer Crime: Issues surrounding the establishment of an international legal regime* (April 2000) INSS Occasional Paper 32 USAF Institute for National Security Studies <<http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>> accessed November 2016

Alexander, K. & Munroe, R. *Cyberpayments: internet and electronic money laundering – Countdown to the year 2000* (1996) 4(2) *Journal of Financial Crime* 156

Alexander, R. *Money Laundering and Terrorist Financing: Time for a combined offence* (2009) 30(7) *Company Lawyer* 200

Alford, D.E. *Anti-Money Laundering Regulations: A Burden on Financial Institutions* (1993-1994) 19 *North Carolina Journal of International Law and Commercial Regulation* 437

All Party Parliamentary Group on Drones *Jemima Stratford QC's Advice* (29 January 2014) <<http://appgdrones.org.uk/jemima-stratford-qcs-advice/>> accessed June 2018

Al Mahroos, R. *Phishing for the answer: Recent Developments in combating phishing* (2007-2008) 3 *ISJLP* 595

Al-Marayati, L. *American Muslim Charities: Easy Targets in the War on Terror* 25 *Pace L. Rev* 321

American Civil Liberties Union *Open letter to Senators* (2001) <<http://www.aclu.org/national-security/letter-senate-urging-rejection-final-version-usa-patriot-act>> accessed November 2016

American Civil Liberties Union *ACLU "Bitterly Disappointed" in House-Senate Joint Passage of Anti-Terrorism Legislation* (12 October 2001) <<http://www.aclu.org/national-security/aclu-bitterly-disappointed-house-senate-joint-passage-anti-terrorism-legislation>> accessed November 2016

American Civil Liberties Union *Khalid Sheik Mohammed Combatant Status Review Tribunal Guantanamo Bay* (10 March 2007) <[https://www.aclu.org/files/pdfs/safe-free/csrt\\_ksm.pdf](https://www.aclu.org/files/pdfs/safe-free/csrt_ksm.pdf)> accessed April 2018

American Civil Liberties Union *National Security Letters FOIA* (2007) <<http://www.aclu.org/national-security/national-security-letters-foia>> accessed November 2016

American Civil Liberties Union *FBI Audit Exposes Widespread Abuse of PATRIOT Powers* (13 March 2008) <[www.aclu.org/safefree/general/34464prs20080313.html](http://www.aclu.org/safefree/general/34464prs20080313.html)> accessed November 2016

American Civil Liberties Union *ACLU sues over Unconstitutional Dragnet Wiretapping Law* (10 July 2008) <[www.aclu.org/safefree/nsaspying/35942prs20080710.html](http://www.aclu.org/safefree/nsaspying/35942prs20080710.html)> accessed November 2016

Amnesty International *Amnesty International website 'blocked in Saudi Arabia'* (25 July 2011) <<https://www.amnesty.org/en/latest/news/2011/07/amnesty-international-website-eblocked-saudi-arabia/>> accessed November 2016

Amnesty International *Raif Badawi* <<https://www.amnesty.org.uk/issues/Raif-Badawi>> accessed November 2016

Amnesty International *Saudi Arabia* <<https://www.amnesty.org/en/countries/middle-east-and-north-africa/saudi-arabia/>> accessed April 2018

Anderson D. *First Report on the Operation of the Terrorist-Asset Freezing etc. Act 2010* (HMSO, December 2011) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/223465/fin\\_sanc\\_report\\_on\\_terrorist\\_asset\\_freezing\\_151211.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/223465/fin_sanc_report_on_terrorist_asset_freezing_151211.pdf)> accessed June 2018

Anderson D. *Fourth Report on the Operation of the Terrorist Asset Freezing etc. Act 2010* (HMSO, March 2015) <<https://www.gov.uk/government/publications/terrorism-and-terrorist-financing-fourth-independent-reviewer-report>> accessed November 2016

Anderson, D. *A Question of Trust: Report of the Investigatory Powers Review* (HMSO, June 2015) <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf>> accessed June 2018

Anderson, D. *Written evidence to the Public Bills Committee IPB 46* (March 2016) <[www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm](http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB46.htm)> accessed November 2016

Anderson D. *Legislation Report of the Bulk Powers Review* Cmd 9326 (HMSO, August 2016) <<https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>> accessed June 2018

Anti-Defamation League *13th Issue of AQAP Inspire Calls for Attacks Against U.S. Airlines* (24 December 2014) <[http://blog.adl.org/extremism/aqap-al-qaeda-inspire-english-magazine-13?\\_ga=1.243425985.530138109.1478458603](http://blog.adl.org/extremism/aqap-al-qaeda-inspire-english-magazine-13?_ga=1.243425985.530138109.1478458603)> accessed November 2016

Anti-Defamation League *New AQAP Inspire Magazine Encourages Lone Wolf Attacks* (21 September 2015) <[http://blog.adl.org/extremism/new-aqap-inspire-magazine-encourages-lone-wolf-attacks?\\_ga=1.54290028.530138109.1478458603](http://blog.adl.org/extremism/new-aqap-inspire-magazine-encourages-lone-wolf-attacks?_ga=1.54290028.530138109.1478458603)> accessed November 2016



Arab News *Cybercrime hit 6.5m in Kingdom last year* (11 August 2016) <<http://www.arabnews.com/node/967966/saudi-arabia>> accessed November 2016

Artingstall, D., Dove, N., Howell, J. & Levi, M. *Drivers & Impacts of Derisking A study of representative views and data in the UK* (John Howell & Co. Ltd. for the Financial Conduct Authority, February 2016) <<https://www.fca.org.uk/news/news-stories/fca-research-issue-de-risking>> accessed November 2016

Ashworth, A. *Case Comment Human rights: Article 8 - right to respect for private life - secret surveillance under powers in Regulation of Investigatory Powers Act 2000* (2010) Crim. L.R. 2010, 11, 868

Attorney General John Ashcroft *Testimony before the Senate Committee on the Judiciary* (Department of Justice, 25 September 2001) <<http://www.justice.gov/archive/ag/testimony/2001/0925AttorneyGeneralJohnAshcroftTestimonybeforetheSenateCommitteeontheJudiciary.htm>> accessed November 2016

Attorney General John Ashcroft *Justice Department Briefing* (Department of Justice, 8 October 2001) <[https://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10\\_08.htm](https://www.justice.gov/archive/ag/speeches/2001/agcrisisremarks10_08.htm)> accessed June 2018

Ayers, A. *The Financial Action Task Force: The war on terrorism will not be fought on the battlefield* (2001-2002) 18 N Y L Sch J Hum Rts 449

Bachus, A.S. *From Drugs to Terrorism: The focus shifts in the international fight against money laundering after September 11 2001* (2004) 21 Arizona Journal of International and Comparative Law 835

Baldwin, F.N. *The financing of terror in the age of the Internet: wilful blindness, greed or a political statement?* (2004) 8(2) Journal of Money Laundering Control 127

Baldwin, F.N. *Money Laundering Countermeasures with Primary Focus upon terrorism and the USA PATRIOT Act 2001* (2003) <[www.imf.org/external/np/leg/sem/2002/cdmfl/eng/baldwin.pdf](http://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/baldwin.pdf)> accessed November 2016

Balls, E. *Written Statement* (Hansard, 10 October 2006) <<https://publications.parliament.uk/pa/cm200506/cmhansrd/vo061010/wmstext/61010m0001.htm>> accessed April 2018

Bank of England *Sandstorm Report* (1991) (Wikileaks, redacted version) <[https://wikileaks.org/wiki/BCCI\\_Sandstorm\\_report,\\_1991](https://wikileaks.org/wiki/BCCI_Sandstorm_report,_1991)> accessed November 2016

Bank for International Settlements *PREVENTION OF CRIMINAL USE OF THE BANKING SYSTEM FOR THE PURPOSE OF MONEY-LAUNDERING* (December 1988) <<https://www.bis.org/publ/bcbssc137.pdf>> accessed April 2018

- Bantenkas, I. *Current Developments: The International Law of Terrorist Financing* (2003) 97 *American Journal of International Law* 315
- Barbot, L.A. *Money Laundering: An International Challenge* (1995) 3 *Tul. Journal Int'l & Comp. Law* 161
- Barnum, D.G. *Warrantless electronic surveillance in national security cases: Lessons from America* (2006) 5 *European Human Rights Law Review* 514
- Barnum, D.G. *Foreign surveillance in the United States: Update* (2008) 5 *European Human Rights Law Review* 633-655
- Basel Committee on Banking Supervision *Risk Management Principles for Electronic Banking* (May 2001) <<http://www.bis.org/publ/bcbs82.pdf>> accessed November 2016
- Basel Committee on Banking Supervision *Customer Due Diligence for Banks* (October 2001) <<http://www.bis.org/publ/bcbs85.pdf>> accessed November 2016
- Beal, K. & Hickman, T. *Beano No More: The EU Charter of Rights After Lisbon* (2011) *JR* 16(2) 113
- Bell, J.L. *Terrorist Abuse of Non-Profits and Charities: A proactive approach to terrorist financing* (2007-8) 17 *Kansas Journal of Law and Public Policy* 450
- Bell, R.E. *The prosecution of computer crime* (2002) 9(4) *Journal of Financial Crime* 308
- Benjamin, V.O. *Interception of Communications and the right to privacy: an evaluation of some provisions of the Regulation of Investigatory Powers Act against the jurisprudence of the European Court of Human Rights* (2007) 6 *European Human Rights Law Review* 637
- Bensted, G. *Terrorist Financing and the Internet: dot com danger* (2012) 21 *Information and Communications Technology Law* 237
- Berger, J.M. *Tailored Online Interventions: The Islamic State's Recruitment Strategy* (Combating Terrorism Center, 23 October 2015) <<https://www.ctc.usma.edu/posts/tailored-online-interventions-the-islamic-states-recruitment-strategy;>> accessed November 2016
- Berkowitz, R. *Packet-sniffers and privacy: Why the no-suspicion-needed standard in the USA PATRIOT Act is unconstitutional* (2002-2003) 7 *Computer L Rev & Tech. J.* 1
- Berman, B. *Combating Terrorist Uses of the Internet* (2005) 99 *American Society of International Law Proceedings* 103
- bin Khalid al-Saud, A. *The Tranquility Campaign: A Beacon of Light in the Dark World Wide Web* (Perspectives on Terrorism Vol. 11 No. 2, 2017) <<http://www.terrorismanalysts.com/pt/index.php/pot/article/view/596/html>> accessed April 2018
- Black's Law Dictionary

- Blackburn, R. *Magna Carta* (British Library) <<https://www.bl.uk/magna-carta/articles/britains-unwritten-constitution>> accessed November 2016
- Blakey, G.R. *Rico: The Genesis of an Idea Trends in Organized Crime* (2006) Vol. 9, No. 8, 9-10
- Blanchard, C. M. RL33533 *CRS Report to Congress Saudi Arabia: Background and U.S. Relations* (20 September 2016) <<https://fas.org/sgp/crs/mideast/RL33533.pdf>> accessed June 2018
- Blasburg, S. *Law and Technology of Security Measures in the Wake of Terrorism* (2002) 8 B. U. J Sci. & Tech L. 721
- Blaut, M.S. *Banking Secrecy – The End of an Era?* (1975) 3 Syracuse Journal of International Law 271
- Blum J. A., Levi, M. Naylor & R.T. Williams, P. (eds.) *Financial Secrecy, Bank Havens and Money Laundering* (1998 – submitted to the UN Office for Drug Control and Crime Prevention) 63
- Boikess, L. *The Unlawful Internet Gambling Enforcement Act: The Pitfalls of Prohibition* (2008) Legislation and Public Policy (12) 151
- Boon K.E., Huq, A. & Lovelace D.C. *Terrorism: Commentary on Security Documents Vol 106 Terrorist Financing and Money Laundering Vol. 107* (Oxford University Press, 2010)
- Boucek, C. *The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia* (Combating Terrorism Center, 15 August 2008) <<https://www.ctc.usma.edu/posts/the-sakinah-campaign-and-internet-counter-radicalization-in-saudi-arabia>> accessed November 2016
- Bozonelos, D. & Stocking, G. *The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com* (2003) 1 JIJIS 88
- Branum, T.L. *President or King - The Use and Abuse of Executive Orders in Modern-Day America* (2002) Journal of Legislation: Vol. 2: Issue. 1, Article 9
- Brand, R. *External Sovereignty and International Law* (1994) 18 Fordham Journal of International Law 1685
- Brenner, S. *Why the law enforcement model is a problematic strategy for dealing with terrorist activity online* (2005) 99 Am Soc’y Int’l L. Proc. 108
- Brenner, S. & Goodman, M. *The emerging consensus on criminal conduct in cyberspace* (2002) 10(2) International Journal of Law and Information Technology 139-223
- Breyer, P. *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR* (2005) 11 European Law Journal 3
- Brisard, J.C. *Terrorism Financing: Roots and Trends of Saudi Terrorism Financing – Report Prepared for the President of the UN Security Council* (Investigative

Project, 19 December 2002)

<<http://www.investigativeproject.org/documents/testimony/22.pdf>> accessed November 2016

Brokenshire, J. *Oral Statement* (Hansard HC Deb c957, 2 April 2014)

Brown, G.D. *Notes on a Terrorism Trial: Preventative Prosecution, 'Material Support' and the Role of the Judge after United States v. Mehanna* (5 April 2013) Boston College Law School Studies Research Paper Series, Research Paper 294

Burnton, S. *Report of the Interception of Communications Commissioner, Review of Directions given under s94 of the Telecommunications Act 1984* (July 2016)

<[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/548013/56208\\_HC33\\_WEB.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/548013/56208_HC33_WEB.pdf)> accessed June 2018

Bryman, A. *Social Research Methods* (2nd Edn. Oxford University Press, 2004)

Cabinet Office *European Council and Woolwich incident: Prime Minister's statement* (3 June 2013) <<https://www.gov.uk/government/speeches/european-council-and-woolwich-prime-ministers-statement>> accessed November 2016

Cabinet Office *Rt. Hon. David Cameron Speech to the NSPCC* (24 July 2013) <<https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action>> accessed November 2016

Cabinet Office *Anti-Corruption Summit: regional and international organisation statements* (12 May 2016) <<https://www.gov.uk/government/publications/anti-corruption-summit-regional-and-international-organisation-statements>> accessed November 2016

Cameron, D. *Oral Statement* (Hansard, 1235, 3 June 2013) <<http://www.publications.parliament.uk/pa/cm201314/cmhansrd/chan10.pdf>> accessed November 2016

Caral, J. *Lessons from ICANN: Is self-regulation of the Internet fundamentally flawed?* (2004) 12 International Journal of Law and Information Technology 1

Carlo, S. *5 Reasons why we need intercept evidence in court* (Liberty Blog, 26 February 2016) <<https://www.libertyhumanrights.org.uk/news/blog/5-reasons-why-we-need-intercept-evidence-court>> accessed November 2016

Cass Weiland, S. *Congress and the Transnational Crime Problem* (1986) 20 International Law 1025

Cassella, S.D. *Terrorism and the Financial Sector: are the right prosecutorial tools being used?* (2004) 7(3) Journal of Money Laundering Control 281

Cassella, S.D. *Reverse Money Laundering* (2003) 7(1) Journal of Money Laundering Control 92

Center on Law and Security *Terrorism Trial Report Card September 11 2001- September 11 2011* (New York University School of Law, 2011)

<<http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf>> accessed November 2016

Central Intelligence Agency *World Fact Book: Saudi Arabia* (2016)  
<<https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html>> accessed November 2016

Chaikin, D. *How effective are suspicious transaction reporting systems?* (2009) 12(3) *Journal of Money Laundering Control* 238

Chaliand, G. & Blin, A. *The History of Terrorism; From Antiquity to al-Qaeda* (1<sup>st</sup> Edn. University of California Press, 2007)

Chargualaf, J. *Terrorism and Cybercrime* (Air Command and Staff College, Air University, May 2008) <<http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA489730>> accessed November 2016

Charity Commission *Counter Terrorism Strategy* (July 2008)  
<<https://www.gov.uk/government/collections/charity-commission-reports-decisions-alerts-and-statements>> accessed April 2018

Charity Commission *Palestinians Relief and Development Fund (Interpal)* (27 February 2009) <<http://www.charity-commission.gov.uk/investigations/inquiry-reports/interpal.asp>> accessed November 2016

Charity Commission *Regulatory Case Report (2010) Muslim Aid*  
<<https://www.gov.uk/government/publications/archived-case-reports/archived-case-reports#regulatory-case-reports-published-in-2010>> accessed November 2016

Charity Commission *Iqra* (22 February 2011) <<https://www.gov.uk/government/publications/archived-inquiry-reports/archived-inquiry-reports#inquiry-reports-published-in-2011>> accessed November 2016

Charity Commission *The Charity Commission's counter-terrorism work* (23 May 2013) <<https://www.gov.uk/government/publications/the-charity-commissions-counter-terrorism-work/the-charity-commissions-counter-terrorism-work>> accessed November 2016

Charity Commission *Charities: how to manage risks when working internationally*, (10 May 2013) <<https://www.gov.uk/guidance/charities-how-to-manage-risks-when-working-internationally>> accessed November 2016

Charity Commission *Charity Commission names further charities under investigation* (5 June 2014) <<https://www.gov.uk/government/news/charity-commission-names-further-charities-under-investigation>> accessed November 2016

Charity Commission *Inquiry Funds raised for charitable purposes and held on charitable trusts in the name of Adeel Ulhaq* (28 July 2016) <<https://www.gov.uk/government/publications/charitable-funds-raised-by-mr-adeel-ul-haq-inquiry-report>> accessed June 2018

Charity Commission *Interim Manager appointed to Muslim Aid* (21 October 2016)  
<<https://www.gov.uk/government/news/interim-manager-appointed-to-muslim-aid>>  
accessed November 2016

Charity Commission *Charities and Terrorism: Compliance Toolkit*  
<<https://www.gov.uk/government/publications/charities-and-terrorism>> accessed  
November 2016

Charity Commission *Safer Giving* <<https://www.gov.uk/government/news/ramadan-safer-giving>> accessed November 2016

Cheung, A. & Weber, R.H. *Internet governance and the responsibility of Internet Service Providers* (2008-9) 26 Wis. Int'l L.J. 403

Chynoweth, P. *Legal research in the built environment: A methodological framework* (Ruddock, L & Knight, A (eds.) *Advanced Research Methods in the Built Environment* 2008, Wiley-Blackwell)

CNET *Homeland Security cuts off Dwolla bitcoin transfers* (14 May 2013)  
<[http://news.cnet.com/8301-13578\\_3-57584511-38/homeland-security-cuts-off-dwolla-bitcoin-transfers/](http://news.cnet.com/8301-13578_3-57584511-38/homeland-security-cuts-off-dwolla-bitcoin-transfers/)> accessed November 2016

Commission Staff Working Document SEC(2007) 1424 *Accompanying document to the Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism (Impact Assessment)* (6 November 2007)  
<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2007:1424:FIN:EN:PDF>> accessed November 2016

Communications and Information Technology Commission *Annual Report 2014*  
<<http://www.citc.gov.sa/en/MediaCenter/Annualreport/Pages/default.aspx>> accessed  
November 2016

*Communication from the Commission to the European Parliament and the Council concerning terrorist recruitment - Addressing the factors contributing to violent radicalisation* COM/2005/0313 (21 September 2005) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0313:FIN:EN:HTML>> accessed November 2016

ComScore *2011 State of Online Banking and Mobile Services* (February 2012)  
<[http://www.comscore.com/Press\\_Events/Presentations\\_Whitepapers/2012/2011\\_State\\_of\\_Online\\_and\\_Mobile\\_Banking](http://www.comscore.com/Press_Events/Presentations_Whitepapers/2012/2011_State_of_Online_and_Mobile_Banking)> accessed November 2016

Congressional Record *Sen. Ron Wyden speech* (GPO S8389, 27 December 2012)  
<<http://www.gpo.gov/fdsys/pkg/CREC-2012-12-27/pdf/CREC-2012-12-27-pt1-PgS8384-2.pdf#page=4>> accessed November 2016

Conway, M. *Terrorism and the Internet: New Media, New Threat?* (2006) 59(2) Parliamentary Affairs 283



Conway, M. *Terrorist 'Use' of the Internet and Fighting Back* (2006) 19 Information & Security 9 <[https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura\\_conway.pdf](https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf)> accessed June 2018

Conway, M. *Terrorism and the Internet: Core Governance and Issues* (2007) 3 Disarmament Forum 23

Cordesman, A. *Saudi Arabia: Friend or Foe in the War on Terror?* (2006) 8(1) Middle East Policy 28

Council of Europe Committee of Ministers *Recommendation No. R 89(9) of the Committee of Ministers to Member States on Computer-related Crime* (13 December 1989) <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCT-MContent?documentId=09000016804f1094>> accessed April 2018

Council of Europe Cybercrime Convention Committee *T-CY Guidance Note #11 Aspects of Terrorism covered by the Budapest Convention*, adopted by the 16th Plenary of the T-CY (14-15 November 2016): <[file:///C:/Users/georg/AppData/Local/Microsoft/Windows/INetCache/IE/U960IG5U/T-CY\(2016\)11\\_GuidanceNote11\\_terrorism\\_V15adopted.docx.pdf](file:///C:/Users/georg/AppData/Local/Microsoft/Windows/INetCache/IE/U960IG5U/T-CY(2016)11_GuidanceNote11_terrorism_V15adopted.docx.pdf)> accessed March 2018

Council of Europe *Global Action on Cybercrime* <<https://www.coe.int/en/web/cybercrime/glacy>> accessed 13 April 2018

Council of Europe *Cybercrime Programme Office* <<https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc->> accessed 13 April 2018

Council of Europe *iPROCEEDS – Targeting crime proceeds on the internet in South Eastern Europe and Turkey* <<https://www.coe.int/en/web/cybercrime/iproceeds>> accessed 13 April 2018

Council of the European Union *Council Decision on Establishing the European Police Office (Europol)* (2009/371/JHA) (6 April 2009) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:121:0037:0066:EN:PDF>> accessed November 2016

Council of the European Union *Council Framework Decision of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime* (2001/500/JHA) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001F0500:EN:HTML>> accessed November 2016

Council of the European Union *EU Human Rights Guidelines on Freedom of Expression Online and Offline* (12 May 2014) <[https://eeas.europa.eu/delegations/documents/eu\\_human\\_rights\\_guidelines\\_on\\_freedom\\_of\\_expression\\_online\\_and\\_offline\\_en.pdf](https://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf)> accessed November 2016

Council on Foreign Relations *Task Force Report Terrorist Financing* (2002) <<http://www.cfr.org/economics/terrorist-financing/p5080>> accessed November 2016

Council on Foreign Relations *Terrorist Financing* (Chairman Maurice R. Greenberg, 2002) <<http://www.cfr.org/terrorist-financing/terrorist-financing/p5080>> accessed November 2016

Cribb, N. *Tracing and confiscating the proceeds of crime* (2003) 11(2) *Journal of Financial Crime* 168

Crimm, N. *High Alert: The Government's war on the financing of terrorism and its implications for donors, domestic charitable organizations and global philanthropy* (2004) 45 *William and Mary Law Review* 1341

Crocker, T.E. & Bellinger, J.B. *New US Anti-Money Laundering Legislation* (1987) 6 *International Financial Law Review* 33

Crown Prosecution Service *15 year old jailed for part in international terror plot* (2 October 2015) <[http://www.cps.gov.uk/news/latest\\_news/15\\_year\\_old\\_jailed\\_for\\_part\\_in\\_international\\_terror\\_plot/](http://www.cps.gov.uk/news/latest_news/15_year_old_jailed_for_part_in_international_terror_plot/)> accessed November 2016

Crown Prosecution Service *R v Forhad Rahman, Adeel Brekke and Kaleem Kristen Ulhaq* (November 2016) <<https://www.cps.gov.uk/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-end-2006>> accessed November 2016

Culture, Media and Sport Committee *Online Safety Volume I* (13 March 2014) <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmcumeds/729/729.pdf>> accessed November 2016

Cutbill, C. *The money launderer, the terrorist financier the charity and the law* (2005) 2 *Private Client Business* 100

Daley, M.J. *Effectiveness of United States and International Efforts to combat international money laundering* (2000) 2000 *St. Louis-Warsaw Transatlantic Law Journal* 175

Daudi, A. *The Invisible Bank: Regulating the Hawala System in India, Pakistan and the United Arab Emirates* (2005) 15 *Indiana International and Comparative Law Review* 619

Davis B. R. *Ending the Cyber-Jihad: Combating Terrorist Exploitation of the Rule of Law and improved tools for Cyber Governance* (2006) 15 *CommLaw Conspectus* 119

Davies, G. & Trigg, G. *Being data retentive: a knee-jerk reaction?* (2006) 11(1) *Communications Law* 18-21

Dean, S.W. *Government surveillance of Internet communications: Pen Register and Trap and Trace Law under the Patriot Act* (2003) 5 *Tul. J. Tech. & Intell. Prop.* 97

DelBianco, S. & Cox, B. *ICANN Internet Governance: Is it working?* (2008) 21 *Pac. McGeorge Global Bus. & Dev. L.J.* 27



Department for Homeland Security *National Strategy to Secure Cyberspace*  
<<https://www.dhs.gov/national-strategy-secure-cyberspace>> accessed April 2018

Department for Homeland Security *Countering Violent Extremism*  
<<https://www.dhs.gov/countering-violent-extremism>> accessed November 2016

Department for Homeland Security *Using 21<sup>st</sup> Century Technology to Defend the Homeland* (19-21 *Securing the Homeland Strengthening the Nation*) (2003)  
<[http://www.dhs.gov/xlibrary/assets/homeland\\_security\\_book.pdf](http://www.dhs.gov/xlibrary/assets/homeland_security_book.pdf)> accessed November 2016

*Developments in the Law: The Law of Cyberspace* (1998-1999) 112 Harvard Law Review 1574

Dicey, A.V. *Introduction to the Law of the Constitution* (8<sup>th</sup> Edn. Oxford Press, 1915)

Dickerson, N.P. *What makes the Internet so special – and why, where, why and by whom should its content be regulated?* (2009) 46 Houston Law Review 61

Dictionary.com *Function Creep* <<http://www.dictionary.com/browse/function-creep>> accessed June 2018

Dieks, M.P. *Computer Network Abuse* (1992-1993) 6 Harvard Journal of Law and Technology 307

Director of National Intelligence *Statement of the Director of National Intelligence, James R. Clapper* (6 June 2013) <<https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information>> accessed April 2018

Director of National Intelligence *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (8 June 2013) <[http://content.govdelivery.com/attachments/USODNI/2013/06/08/file\\_attachments/217069/Facts%2Bon%2Bthe%2BCollection%2Bof%2BIntelligence%2BPursuant%2Bto%2BSection%2B702.pdf](http://content.govdelivery.com/attachments/USODNI/2013/06/08/file_attachments/217069/Facts%2Bon%2Bthe%2BCollection%2Bof%2BIntelligence%2BPursuant%2Bto%2BSection%2B702.pdf)> accessed November 2016

Donohue, L.K. *Anti-Terrorist Finance in the United Kingdom and the United States* (2005-6) 27 Mich. J Int'l L. 303

Donohue, L.K. *Anglo-American Privacy and Surveillance* (2005-6) 96 Journal of Criminal Law and Criminology 1059

Donohue, L.K. *The Cost of Counterterrorism: Power, Politics and Liberty* (1<sup>st</sup> Edn. Cambridge University Press, 2008)

Doyle, C. R40887 *CRS Report to Congress National Security Letters: Proposed Amendments in the 111<sup>th</sup> Congress* (27 December 2010)  
<<https://fas.org/sgp/crs/intel/R40887.pdf>> accessed November 2016

Draper, S. *Retroactive Immunity: A Legislative Faux Pas?* (2009) *BYU Prelaw Review*, Vol. 23, 70-71

Drozдова, E.A. *CISAC Report: Civil liberties and security in cyberspace* (2000) <[https://cisac.fsi.stanford.edu/publications/civil\\_liberties\\_and\\_security\\_in\\_cyberspace](https://cisac.fsi.stanford.edu/publications/civil_liberties_and_security_in_cyberspace)> accessed June 2018

Dutton, W.H., Dopatka, A. Hills, M., Law, G & Nash, V. *Freedom of Connection, Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet* (UNESCO, 2011) <<http://unesdoc.unesco.org/images/0019/001915/191594e.pdf>> accessed April 2018

Economic Policy Journal *US Government seizes assets of another Bitcoin Exchange; Firm President Arrested* (28 May 2013) <<http://www.economicpolicyjournal.com/2013/05/us-government-seizes-assets-of-another.html>> accessed November 2016

Edwards, L. *From Child Porn to China, in one Cleanfeed* 3(3) *SCRIPTed* 174 (September 2006) <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1128062](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1128062)> accessed June 2018

Egmont Group *List of Members* <<https://www.egmontgroup.org/en/membership/list>> accessed April 2018

Egmont Group *Financial Intelligence Units* <<https://egmontgroup.org/en/content/financial-intelligence-units-fius>> accessed April 2018

Elagab, O. *Control of Terrorist Funds and the banking system* (2006) 21(1) *Journal of International Banking Regulation* 38

Electoral Commission *EU referendum results* (June 2016) <<http://www.electoral-commission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information>> accessed November 2016

Electronic Frontier Foundation *Analysis of the Provisions of the USA PATRIOT Act that relate to online activities Title III section B* (31 October 2001) <[http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031\\_eff\\_usa\\_patriot\\_analysis.php](http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php)> accessed November 2016

Electronic Frontier Foundation *Ten Years After the Patriot Act, a Look at Three of the Most Dangerous Provisions Affecting Ordinary Americans* (12 October 2011) <<https://www.eff.org/deeplinks/2011/10/ten-years-later-look-three-scariest-provisions-usa-patriot-act>> accessed November 2016

Electronic Frontier Foundation *EU Court of Justice: Social Networks Can't Be Forced to Monitor and Filter to Prevent Copyright Infringement* (17 February 2012) <<https://www.eff.org/deeplinks/2012/02/eu-court-justice-social-networks>> accessed November 2016

Electronic Frontier Foundation *The Cost of Censorship in Libraries: 10 Years Under the Children's Internet Protection Act* (4 September 2013) <<https://www.eff.org/deeplinks/2013/09/cost-censorship-libraries-10-years-under-childrens-internet-protection-act>> accessed November 2016

El-Guindy, M. *Cybercrime in the Middle East* (ISSA Journal, 2008) <<http://www.ask-pc.com/lessons/CYBERCRIME-MIDDLE-EAST.pdf>> accessed November 2016

Elnaim, B.M.E. *Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future* (2013) Information and Knowledge Management Vol.3, No.12, 17

EPIC *Foreign Intelligence Surveillance Act Court Orders 1979-2012* <[http://epic.org/privacy/wiretap/stats/fisa\\_stats.html](http://epic.org/privacy/wiretap/stats/fisa_stats.html)> accessed November 2016

European Commission *Digital Agenda: Commission refers UK to Court over privacy and personal data protection* (Europa.eu, 30 September 2010) <[http://europa.eu/rapid/press-release\\_IP-10-1215\\_en.htm](http://europa.eu/rapid/press-release_IP-10-1215_en.htm)> accessed April 2018

European Commission *Anti-Money Laundering: Stronger rules to respond to new threats* (Europa.eu, 5 February 2013) <[http://europa.eu/rapid/press-release\\_IP-13-87\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-13-87_en.htm?locale=en)> accessed November 2016

European Commission *Questions and Answers: Money Laundering Directive Fact-sheet* (Europa.eu, 5 July 2016) <[http://europa.eu/rapid/press-release\\_MEMO-16-2381\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-2381_en.htm)> accessed November 2016

European Commission *Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering* (Europa.eu, 5 July 2016) <[http://europa.eu/rapid/press-release\\_IP-16-2380\\_en.htm](http://europa.eu/rapid/press-release_IP-16-2380_en.htm)> accessed November 2016

European Parliament *European Parliament resolution of 22 November 2012 on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations* (2012/2881(RSP), European Parliament, 2012) <<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0451&language=EN&ring=P7-RC-2012-0498>> accessed November 2016

European Parliament *MEPs call for suspension of EU-US bank data deal in response to NSA snooping* (23 October 2013) <http://www.europarl.europa.eu/news/en/press-room/20131021IPR22725/meps-call-for-suspension-of-eu-us-bank-data-deal-in-response-to-nsa-snooping> accessed June 2018

European Parliament *Parliament toughens up anti-money laundering rules* (European Parliament, 11 March 2014) <<http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38110/html/Parliament-toughens-up-anti-money-laundering-rules>> accessed November 2016

European-Saudi Organisation for Human Rights *Law of terrorism crimes and its financing* <[http://www.esohr.org/en/?page\\_id=788](http://www.esohr.org/en/?page_id=788)> accessed November 2016

European Scrutiny Committee *The EU Charter of Fundamental Rights in the UK: a state of confusion* (HMSO, Forty Third Report of Session 2013-14) <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmeuleg/979/979.pdf>> accessed November 2016

European Union *Convention drawn up on the basis of Article K.3 of the Treaty on the European Union, on the Establishment of a European Police Office (Europol Convention)* (Official Journal 316, 27 November 1995) <[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41995A1127\(01\):EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:41995A1127(01):EN:HTML)> accessed November 2016

European Union *EU List of Terrorist Organisations* (Council Common Position 2006/380/CFSP, 29 May 2006) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006E0380>> accessed April 2018

European Union *Agreement between the European Union and Japan on mutual legal assistance in criminal matters* (European Union, 12 February 2010) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0020:0035:EN:PDF>> accessed April 2018

Exten, S.E. *Major Developments in Financial Privacy Law 2006: The SWIFT Database incident and updates to the Gramm-Leach-Bailey and Fair Credit Reporting Acts* (2007-2008) 3 I.S.J.L.P. 649

Farr, C.B. *Witness Statement of Charles Blandford Farr on behalf of the Respondents* (Exhibit CF1) in cases IPT/13/92/CH *Privacy International* and (1) *The Secretary of State for Foreign and Commonwealth Affairs* (2) *The Secretary of State for the Home Department* (3) *The Secret Intelligence Service* (4) *The Security Service* (5) *The Government Communications Headquarters* (6) *The Attorney General*; IPT/13/77/H *Liberty* and (1) *The Government Communication Headquarters* (2) *The Secret Intelligence Service* (3) *The Security Service*; IPT/L3/168-173/H (1) *American Civil Liberties Union* (2) *Canadian Civil Liberties Association* (3) *Egyptian Initiative for Personal Rights* (4) *Hungarian Civil Liberties Union* (5) *Irish Council for Civil Liberties* (6) *Legal Resources Centre* and (1) *The Government Communication Headquarters* (2) *The Secret Intelligence Service* (3) *The Security Service*; IPT/13/194/CH *Amnesty International Limited* and (1) *The Security Service* (2) *The Secret Intelligence Service* (3) *The Government Communications Headquarters* (4) *The Secretary of State for Foreign and Commonwealth Affairs*; IPT/13/204/CH *Bytes for All* and (1) *The Secretary of State for Foreign and Commonwealth Affairs* (2) *The Secretary of State for the Home Department* (3) *The Secret Intelligence Service* (4) *The Security Service* (5) *The Government Communications Headquarters* (6) *The Attorney General* (16 May 2014) <<https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/witness-st-of-charles-blandford-farr.pdf>> accessed November 2016

FBI Countering Violent Extremism *FBI Launches New Awareness Program for Teens* (8 February 2016) <<https://www.fbi.gov/news/stories/countering-violent-extremism>> accessed November 2016

FBI Intelligence Assessment *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity* (24 April 2012) <[http://www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf)> accessed November 2016

Federal Bureau of Investigation *'East African Embassy Bombings'* <<https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings>> accessed November 2016

Federal Bureau of Investigation *FBI's 9/11 Chronology, Part 2 of 2,158* <<http://vault.fbi.gov/9-11%20Commission%20Report/9-11-chronology-part-02-of-02/view>> accessed November 2016

Federal Bureau of Investigation *Operation Phish Phry* (7 October 2009) <[http://www.fbi.gov/news/stories/2009/october/phishphry\\_100709](http://www.fbi.gov/news/stories/2009/october/phishphry_100709)> accessed November 2016

Federal Bureau of Investigation *Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business* (9 November 2011) <<https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business>> accessed April 2018

Federal Bureau of Investigations Cybercrime Division *Key Priorities* <<http://www.fbi.gov/about-us/investigate/cyber/cyber>> accessed November 2016

Federal Reserve Bank *Supporting Statement for the Suspicious Activity Report by Depository Institutions* <[http://www.federalreserve.gov/reportforms/formsreview/FR2230\\_20120720\\_omb.pdf](http://www.federalreserve.gov/reportforms/formsreview/FR2230_20120720_omb.pdf)> accessed November 2016

Feingold, R. (Sen.) *Congressional Record* (Government Publishing Office, Volume 147, Issue 144 S11020-S11023, 25 October 2001) <<http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi>> accessed November 2016

Ferguson, G. & Wadham, J. *Privacy and Surveillance: A review of the Regulation of Investigatory Powers Act 2000* (2003) *European Human Rights Law Review* 101

Ferrari, E. *Deep Freeze: Islamic Charities and the War on Terror* (2004-2005) 7 *Scholar* 205

Financial Action Task Force *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* <<http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>> accessed April 2018



Financial Action Task Force *International Best Practices - Combating the Abuse of Non-Profit Organisations* (11 October 2002) <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/11%20FATF%20SRIX%20BPP%20SRVIII%20October%202003%20-%20COVER%202012.pdf>> accessed November 2016

Financial Action Task Force *Third Mutual Evaluation Report on Anti-Money Laundering and Combating the Financing of Terrorism: The United States of America* (23 June 2006) <<http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20US%20full.pdf>> accessed April 2018

Financial Action Task Force *Third Mutual Evaluation report on Anti Money Laundering and Combating the Financing of Terrorism: The United Kingdom of Great Britain and Northern Ireland* (29 June 2007) <<http://www.fatf-gafi.org/publications/mutualevaluations/documents/mutualevaluationoftheunitedkingdom-follow-up-report.html>> accessed April 2018

Financial Action Task Force *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* (18 June 2008) <<http://www.fatf-gafi.org/documents/documents/moneylaunderingterroristfinancingvulnerabilitiesofcommercialwebsitesandinternetpaymentsystems.html>> accessed November 2016

Financial Action Task Force *Annual Report (2009-2010)* <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/fatfannualreport2009-2010.html>> accessed April 2018

Financial Action Task Force *Global Money Laundering and Terrorist Financing Threat Assessment* (July 2010) <<http://www.fatf-gafi.org/publications/methodsand-trends/documents/globalmoneylaunderingterroristfinancingthreatassessment.html>> accessed April 2018

FATF *Guidance for a risk-based approach: Prepaid Cards, Mobile Payments and Internet-based Payment Services* (June 2013) <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf>> accessed November 2016

Financial Action Task Force *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (June 2014) <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>> accessed November 2016

Financial Action Task Force *Combating the Abuse of Non-Profit Organisations - International Best Practices* (June 2015) <<http://www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf>> accessed November 2016

Financial Action Task Force *Financing of the terrorist organization Islamic State in Iraq and the Levant (ISIL)* (2015) <[www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf)> accessed November 2016

Financial Action Task Force *Outcomes of the Plenary meeting of the FATF, Busan Korea* (22–24 June 2016) <<http://www.fatf-gafi.org/publications/fatfgeneral/documents/plenary-outcomes-june-2016.html>> accessed November 2016

Financial Action Task Force *Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies* <<http://www.fatf-gafi.org/countries/#high-risk>> accessed April 2018

Financial Crime Enforcement Network (FinCEN) *History of Anti-Money Laundering Laws* <<https://www.fincen.gov/history-anti-money-laundering-laws>> accessed April 2018

FinCEN *Pending Rulemaking* <<https://www.fincen.gov/resources/statutes-regulations/federal-register-notices/pending-rulemakings>> accessed April 2018

FinCEN *A Survey of Electronic Cash, Electronic Banking and Internet Gaming* (2000) <<https://www.fincen.gov/sites/default/files/shared/e-cash.pdf>> accessed June 2018

FinCEN *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System* (2006) <<https://www.fincen.gov/reports-congress-0>> accessed June 2018

FinCEN *Annual Report 2010* <[http://www.fincen.gov/news\\_room/rp/files/annual\\_report\\_fy2010.pdf](http://www.fincen.gov/news_room/rp/files/annual_report_fy2010.pdf)> accessed November 2016

FinCEN *Annual Report 2011* <[https://www.fincen.gov/sites/default/files/shared/annual\\_report\\_fy2011.pdf](https://www.fincen.gov/sites/default/files/shared/annual_report_fy2011.pdf)> accessed April 2018

FinCEN *By the Numbers Report Issue 16* (May 2011) <<https://www.fincen.gov/news-room/sar-technical-bulletins>> accessed April 2018

FinCEN *FinCEN's reports going paperless* (24 February 2012) <[http://www.fincen.gov/news\\_room/nr/html/20120223.html](http://www.fincen.gov/news_room/nr/html/20120223.html)> accessed November 2016

FinCEN *By the Numbers Report Issue 17* (May 2012) <<https://www.fincen.gov/news-room/sar-technical-bulletins>> accessed April 2018

FinCEN *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (18 March 2013) <<https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>> accessed April 2018

FinCEN *SAR Stats Technical Bulletin* (October 2015) <[https://www.fincen.gov/news\\_room/rp/files/SAR02/SAR\\_Stats\\_2\\_FINAL.pdf](https://www.fincen.gov/news_room/rp/files/SAR02/SAR_Stats_2_FINAL.pdf)> accessed April 2018

FinCEN SAR Stats <[https://www.fincen.gov/news-room/sar-technical-bulletins?field\\_date\\_release\\_value=&field\\_date\\_release\\_value\\_1=&field\\_tags\\_sar\\_report\\_target\\_id=687](https://www.fincen.gov/news-room/sar-technical-bulletins?field_date_release_value=&field_date_release_value_1=&field_tags_sar_report_target_id=687)> accessed April 2018

Financial Conduct Authority *Anti-money laundering annual report 2012/13* (July 2013) <<https://www.fca.org.uk/publication/corporate/anti-money-laundering-report.pdf>> accessed November 2016

Financial Conduct Authority *FCA fines Guaranty Trust Bank (UK) Ltd £525,000 for failures in its anti-money laundering controls* (9 August 2013) <<https://www.fca.org.uk/news/press-releases/fca-fines-guaranty-trust-bank-uk-ltd-%C2%A3525000-failures-its-anti-money-laundering>> accessed November 2016

Financial Conduct Authority *FCA fines Barclays £72 million for poor handling of financial crime risks* (26 November 2015) <<https://www.fca.org.uk/news/press-releases/fca-fines-barclays-%C2%A372-million-poor-handling-financial-crime-risks>> accessed November 2016

Financial Fraud Action UK *Year-end 2015 fraud update: Payment cards, remote banking and cheque* (17 March 2016) <<https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/downloads-7-3085-2015-year-end-fraud-update-report.pdf>> accessed November 2016

Financial Fraud Action UK *Fraud: The Facts 2016* <<https://www.financialfraudaction.org.uk/fraudfacts16/>> accessed November 2016

Financial Services Authority *Carol Sergeant, Director of Banks and Building Societies, Financial Services Authority* (29 March 2000) <<http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2000/sp46.shtml>> accessed November 2016

Financial Services Authority *The Money Laundering Theme: Tackling our new responsibilities* (July 2001) <[http://www.fsa.gov.uk/pubs/other/money\\_laundering.pdf](http://www.fsa.gov.uk/pubs/other/money_laundering.pdf)> accessed November 2016

Financial Services Authority *Final Notice Coutts and Company* (Reference Number 122287) (23 March 2012) <<https://www.fca.org.uk>> accessed November 2016

Fisher, J. *Memorandum to the European Union Committee* (HMSO, 20 February 2009) <<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/132we11.htm>> accessed November 2016

Fletcher, N. *Challenges for regulating financial fraud in cyberspace* (2007) 14(2) *Journal of Financial Crime* 190

Folendorf, C.L. *Breaking Terror's Bank without Breaking the Law: A comment on the USA PATRIOT Act and the United States War Against Terrorism* (2003-2004) 23 *Journal of National Association of Administrative Law Judges* 481



Forbes Magazine *After Liberty Reserve Shutdown is Bitcoin next?* (31 May 2013) <<http://www.forbes.com/sites/petercohan/2013/05/29/after-liberty-reserve-shut-down-is-bitcoin-next/>> accessed November 2016

Foreign Office *Foreign Secretary responds to Intelligence and Security Committee* (17 July 2013) <<https://www.gov.uk/government/news/foreign-secretary-responds-to-intelligence-and-security-committee-statement-on-gchq>> accessed November 2016

Foundation for Information Policy Research *UK Information Commissioner Study Project: Privacy and Law Enforcement Paper Number 5* (February 2004) <[www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/conclusion\\_and\\_policy\\_options.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/conclusion_and_policy_options.pdf)> accessed November 2016

Franklin, A. Schorr L. & Shapiro D. *Racketeering Influenced Corrupt Organizations* (2008) 45 American Criminal Law Review 921

Freedom House *Saudi Arabia Freedom on the Net 2011* <<https://freedomhouse.org/report/freedom-net/2011/saudi-arabia>> accessed November 2016

Freedom House *Freedom on the Net 2012: Saudi Arabia* <<https://freedomhouse.org/report/freedom-net/2012/saudi-arabia>> accessed November 2016

Freedom House *Freedom on the Net: Saudi Arabia* (2015) <<https://freedomhouse.org/report/freedom-net/2015/saudi-arabia>> accessed November 2016

Gambling Commission *Money Laundering: The Prevention of money laundering and the financing of terrorism – Guidance for remote and non-remote casinos* (December 2011): <<http://www.gamblingcommission.gov.uk/PDF/AML/Prevention-of-money-laundering-and-combating-the-financing-of-terrorism.pdf>> accessed April 2018

Gardella, A. *The fight against the financing of terrorism: Between Judicial and Regulatory co-operation* (2003-2004) 6 Stud. Int'l Fin. Econ & Tech. L. 109

Gardner, K.L. *Fighting Terrorism the FATF Way* (2007) 13(3) Global Governance 325

General Secretariat of the Council of the EU *Background: The Lisbon Treaty's impact on the Justice and Home Affairs (JHA) Council: More co-decisions and new working structures* (December 2009) <[http://www.consilium.europa.eu/uedocs/cms\\_data/docs/pressdata/en/ec/111615.pdf](http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/111615.pdf)> accessed November 2016

Gentle, S. *Legislative Comment: Proceeds of Crime Act 2002* (2003) Compliance Officer Bulletin 12(Dec/Jan) 1-29

Gillespie, A.A. *Regulation of Internet surveillance* (2009) European Human Rights Law Review 4, 552-565

- Gilmore, W.C. *International Efforts to Combat Money Laundering* (1992) 18 Commonwealth Law Bulletin 1129
- Goodman, M. *Future Crimes* (1st Edn. Transworld Publishers, 2015)
- Gouvin, E.J. *Bringing out the big guns: The USA PATRIOT Act, Money Laundering and the war on Terrorism* (2003) 55 Baylor Law Review 956
- Government Accounting Office *Internet Gambling: An Overview of the Issues* (December 2002) <<http://www.gao.gov/new.items/d0389.pdf>> accessed November 2016
- Greer, S. *Human Rights and the Struggle Against Terrorism in the United Kingdom* (2008) 2 European Human Rights Law Review 163
- Groden, C. M. *These Countries Have the World's Worst Internet Access* (Fortune.com, 6 October 2015) <<http://fortune.com/2015/10/06/worst-internet-access/>> accessed 15 October 2016
- Guiora, A.N. & Field, B.J. *Using and Abusing the Financial Markets: Money Laundering as the Achilles' Heel of Terrorism* (2007-8) 29 U. Pa. J. Int'l L. 59
- Gurulé, J. *The Demise of the U.N. Economic Sanctions Regime to deprive terrorists of funding* (2009) 41 Case W. Res J. Int'l L. 19
- Gurulé, J. *Unfunding Terror: The Legal Response to the Financing of Global Terrorism* (1<sup>st</sup> Edn. Edward Elgar, 2008)
- Gurulé, J. & Corn, G.S. *Principles of Counter-Terrorism Law* (1<sup>st</sup> Edn. Thompson-West, 2011)
- Gurulé, J. *The 1988 U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances – A Ten Year Perspective: Is International Cooperation Merely Illusory?* (1998-1999) 22 Fordham International Law Journal 75
- Haglund, R.H. *Applying Pen Register and Trap and Trace devices to Internet communications: As technology changes, is Congress or the Supreme Court best suited to protect Fourth Amendment expectations of privacy?* (2002-2003) 5 Vand. J. Ent. L & Prac. 137
- Hamblett, M. *Saudi Charity Dropped from Suit over Sept. 11 Attacks* (28 September 2005) New York Law Journal <<https://archive.li/iXoRG>> accessed June 2018
- Hamilton, L. *Regulation of the Internet: An impossible task?* (2010) 4 Galway Student L. Rev. 33
- Hardister, A.D. *Can We Buy a Peace on Earth: The Price of Freezing Terrorist Assets in a Post-September 11 World* (2002) 28 N.C. J. Int'l L. & Com. Reg. 605
- Harrison K. & Ryder N. *The Law Relating to Financial Crime in the United Kingdom* (2<sup>nd</sup> Edn. Routledge, 2016)
- Haynes, A. *The Wolfsberg Principles: An Analysis* (2004) 7(3) Journal of Money Laundering Control 207

Henning, A. C., Bazan, E. B., Doyle, C. & Liu, E. C. R40980 *CRS Report to Congress – Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization* (23 December 2009) <[https://digital.library.unt.edu/ark:/67531/metadc627051/m1/1/high\\_res\\_d/R40980-2009Dec23.pdf](https://digital.library.unt.edu/ark:/67531/metadc627051/m1/1/high_res_d/R40980-2009Dec23.pdf)> accessed November 2016

Hett, W. *Digital Currencies and the Financing of Terrorism* (2008-9) 15 *Richmond Journal of Law and Technology* 1

Hinnen, T. *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet* (2004) 5 *Columbia Science and Technology Law Review* 5

HM Government *Prevent Strategy* <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/97976/prevent-strategy-review.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf)> accessed November 2016

HM Revenue & Customs *Money Laundering Regulations: Money Services Business registration* (February 2014) <<https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration>> accessed November 2016

HM Treasury *Combating the financing of terrorism – A Report on UK Action* (October 2002) <[http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating\\_terrorism.pdf](http://webarchive.nationalarchives.gov.uk/20120306211630/http://www.hm-treasury.gov.uk/d/combating_terrorism.pdf)> accessed November 2016

HM Treasury *The Financial Challenge to crime and terrorism* (February 2007) <[http://webarchive.nationalarchives.gov.uk/20120704153538/http://www.hm-treasury.gov.uk/d/financialchallenge\\_crime\\_280207.pdf](http://webarchive.nationalarchives.gov.uk/20120704153538/http://www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf)> accessed April 2018

HM Treasury *Transposition of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016

HM Treasury and Home Office consultation summary responses *Review of the Safeguards to Protect the Charitable Sector (England and Wales) from terrorist abuse* (December 2007) <<http://webarchive.nationalarchives.gov.uk/+/http://www.homeoffice.gov.uk/documents/cons-2007-protecting-charities/cons-2007-charities-responses?view=Binary>> accessed November 2016

Home Affairs Committee *Memorandum to the Home Affairs Committee Post Legislative Scrutiny of the Terrorism Act 2006* Cm8186 (HMSO, September 2011) <<http://www.official-documents.gov.uk/document/cm81/8186/8186.pdf>> accessed November 2016

Home Affairs Select Committee *E-Crime Fifth Report of Session 2013-14* (HMSO, 17 July 2013) <<http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>> accessed November 2016

Home Office *Legislation Against Terrorism* Cm4178 (HMSO, December 1998)

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/265689/4178.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/265689/4178.pdf)> accessed April 2018

Home Office *Written Evidence: All Party Parliamentary Internet Group Inquiry on the Computer Misuse Act* (2004) <<http://www.apcomms.org.uk/apig/archive/activities-2004/computer-misuse-inquiry/computer-misuse-inquiry-written-evidence.html>> accessed November 2016

Home Office *Report of the Official Account of the Bombings in London on 7th July 2005* HC1087 (HMSO, 11 May 2006) <<https://www.gov.uk/government/publications/report-of-the-official-account-of-the-bombings-in-london-on-7th-july-2005>> accessed November 2016

Home Office *Challenge Online Terrorism and Extremism* (7 April 2011) <<https://www.gov.uk/government/news/challenge-online-terrorism-and-extremism>> accessed April 2018

Home Office *Channel Guidance* (2012) <<https://www.gov.uk/government/publications/channel-guidance>> accessed November 2016

Home Office *Spending Round: security the foundation of prosperity says Home Secretary* (26 June 2013) <<https://www.gov.uk/government/news/spending-round-security-the-foundation-of-prosperity-says-home-secretary>> accessed November 2016

Home Office *CONTEST, the United Kingdom's strategy for countering terrorism: annual report for 2014* (23 March 2015) <<https://www.gov.uk/government/publications/contest-uk-strategy-for-countering-terrorism-annual-report-for-2014>> accessed June 2018

Home Office Factsheet *Investigatory Powers Bill: Internet Connection Records* (30 October 2015) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530556/Internet\\_Connection\\_Records\\_factsheet.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530556/Internet_Connection_Records_factsheet.pdf)> accessed November 2016

Home Office *Investigatory Powers Bill* (1 March 2016) <[www.gov.uk/government/collections/investigatory-powers-bill](http://www.gov.uk/government/collections/investigatory-powers-bill)> accessed November 2016

Home Office *Bulk Personal Data Factsheet for the Investigatory Powers Bill* (4 March 2016) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/530548/BPD\\_Factsheet.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/530548/BPD_Factsheet.pdf)> accessed November 2016

Home Office *Action Plan for anti-money laundering and counter-terrorist finance* (April 2016) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/517992/6-2118-Action\\_Plan\\_for\\_Anti-Money\\_Laundering\\_web\\_.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering_web_.pdf)> accessed November 2016

Home Office *Proscribed Terrorist Organisations* (15 July 2016) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/538297/20160715-Proscription-website-update.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/538297/20160715-Proscription-website-update.pdf)> accessed November 2016

Home Office *CONTEST: The United Kingdom's Strategy for Countering Terrorism: Annual Report for 2015* Cm9310 (26 July 2016) <<https://www.gov.uk/government/publications/contest-uk-strategy-for-countering-terrorism-annual-report-for-2015>> accessed November 2016

Home Office *Impact Assessment of the Fourth Money Laundering Directive* (15 September 2016) <<https://www.gov.uk/government/consultations/transposition-of-the-fourth-money-laundering-directive>> accessed November 2016

Home Office *Consolidated List of Targets* <<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>> accessed November 2016

House of Lords European Union Committee 19<sup>th</sup> Report of Session 2008-9 *Money Laundering and the Financing of Terrorism Volume II: Evidence* (HMSO, July 2009) <<http://www.publications.parliament.uk/pa/ld200809/ldselect/ldeucom/132/132i.pdf>> accessed November 2016

House of Lords Select Committee on the Constitution 2<sup>nd</sup> Report of 2008-9 *Surveillance: Citizens and the State* (Volume I, HMSO January 2009) <<https://publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf>> accessed November 2016

House of Lords Science and Technology Select Committee 5<sup>th</sup> Report of 2006-7 *Personal Internet Security* (HMSO 10 August 2007) <<http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>> accessed November 2016

Hund, B. *Disappearing Safeguards: FISA non-resident alien 'loophole' is unconstitutional* (2007) 15 Cardozo Journal of International & Computer Law 169

Human Rights Watch *Precarious Justice: Arbitrary Detention and Unfair Trials in the Deficient Criminal Justice System of Saudi Arabia* (2008) <[http://www.hrw.org/sites/default/files/reports/saudijustice0308\\_1.pdf](http://www.hrw.org/sites/default/files/reports/saudijustice0308_1.pdf)> accessed November 2016

Human Rights Watch *Saudi Arabia: Website Editor Facing Death Penalty* (22 December 2012) <<https://www.hrw.org/news/2012/12/22/saudi-arabia-website-editor-facing-death-penalty>> accessed November 2016

Hummel, M.L. *Internet Terrorism* (2008) 2 Homeland Security Review 117

Husain, A. *Framing the International Standard on the global flow of information on the Internet* (2008-9) 3 Interdisc Journal of Human Rights Law 35

Hunt, J. *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them* (2011) 20(2) Information & Communications Technology Law 133

Hunter, P. *BT's bold pioneering child porn block wins plaudits amid Internet censorship concerns* (2004) 9 Computer Law and Security 4-5

IHS Markit *Islamic State Monthly Revenue Drops to \$56 million, IHS Says* (18 April 2016) <<http://press.ihs.com/press-release/aerospace-defense-security/islamic-state-monthly-revenue-drops-56-million-ihs-says>> accessed November 2016

Information Commissioner *Study Project: Privacy and Law Enforcement* (February 2004) <[http://www.ico.gov.uk/upload/documents/library/corporate/research\\_and\\_reports/technology\\_and\\_privacy.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/technology_and_privacy.pdf)> accessed November 2016

Ingber, A. *Cybercrime Control: Will Websites ever be accountable for the legal activities they profit from?* (2011-2012) 18 Cardozo Journal of Law and Gender 423

Intelligence and Security Committee *Intelligence and Security Committee Annual Report 2012-13* (HC 547) <<http://isc.independent.gov.uk/committee-reports/annual-reports>> accessed November 2016

Intelligence and Security Committee/Rt. Hon. Sir Malcolm Rifkind MP *Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme* (17 July 2013) <<http://isc.independent.gov.uk/news-archive>> accessed November 2016

Intelligence and Security Committee *Privacy and Security Inquiry - Call for Evidence* (11 December 2013) <<http://isc.independent.gov.uk/news-archive/11december2013>> accessed November 2016

Interception of Communications Commissioner's Office *2013 Annual Report of the Interception of Communications Commissioner* <<http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf>> accessed November 2016

International Monetary Fund *Factsheet: The IMF and the Fight Against Money Laundering and Terrorist Financing* (10 September 2010) <<http://www.imf.org/external/np/exr/facts/aml.htm>> accessed November 2016

International Monetary Fund *Members* <<http://www.imf.org/external/np/sec/memdir/members.htm>> accessed November 2016

International Monetary Fund *IMF Role in Anti Money Laundering/Counter-Terrorist Financing* <<http://www.imf.org/external/np/exr/facts/aml.htm>> accessed November 2016

International Telecommunications Union *Understanding Cybercrime: A Guide for Developing Countries* (2009) <<https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf>> accessed April 2018

International Telecommunications Union *World Conference on International Telecommunications (WCIT-12)* (3-14 December 2012) <<http://www.itu.int/en/wcit-12/Pages/default.aspx>> accessed November 2016



International Telecommunications Union *International Telecommunication Regulations* (14 December 2012) <<https://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf>> accessed November 2016

International Telecommunications Union *Signatories of the Final Acts* <<http://www.itu.int/osg/wcit-12/highlights/signatories.html>> accessed November 2016

Internet Crime Complaint Center (“IC3”) *2011 Internet Crime Report* <[http://www.ic3.gov/media/annualreport/2011\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf)> accessed November 2016

Internet Crime Complaint Center (“IC3”) *2015 Internet Crime Report* <<https://www.ic3.gov/default.aspx>> accessed November 2016

Internet Gaming Prohibition Act 1999 (H.R. 3215, defeated before Congress) <<http://www.govtrack.us/congress/bill.xpd?bill=h106-3125>> accessed November 2016

Internet Live Stats *Internet Users* (2016) <<http://www.internetlivestats.com/internet-users/>> accessed November 2016

Internet Live Stats *Saudi Arabia Internet Users* <<http://www.internetlivestats.com/internet-users/saudi-arabia/>> accessed November 2016

Internet Live Stats *Google Search Statistics* <<http://www.internetlivestats.com/google-search-statistics/>> accessed November 2017

Internet Watch Foundation *History* <<https://www.iwf.org.uk/about-iwf/iwf-history>> accessed November 2016

Internet Watch Foundation *Memorandum of Understanding* (October 2004) <<https://www.iwf.org.uk/what-we-do/how-we-assess-and-remove-content/laws-and-assessment-levels/memorandum-of-understanding>> accessed April 2018

Internet Watch Foundation *Annual Report 2012* <<https://www.iwf.org.uk/report/2012-annual-report>> accessed April 2018

INTERPOL *Preventing Internet radicalization of youth requires global police network, INTERPOL Chief tells police summit - Secretary General warns of threat posed by 'skyrocketing' number of extremist websites* (21 September 2010) <<http://www.interpol.int/public/ICPO/PressReleases/PR2010/PR072.asp>> accessed November 2016

Intuit *One Third of Consumers Now Using Online Banking Tools To Manage Finances* (19 October 2010) <[http://about.intuit.com/about\\_intuit/press\\_room/press\\_release/articles/2010/OnlineBankingToolsToManageFinances.html](http://about.intuit.com/about_intuit/press_room/press_release/articles/2010/OnlineBankingToolsToManageFinances.html)> accessed November 2016

Investigatory Powers Tribunal *Interception of Communications Commissioner's Annual Report for 2001* HC 1243 (HMSO, 31 October 2002) <<http://www.ipt-uk.com/docs/inter-comm-report-2001.pdf>> accessed November 2016

Jabbour, V. *Interception of Communications - 1: Private Rights and Public Policy* (1999) 15 Computer Law and Security Report 6

Jacobs, J.B. *Mobsters, Unions, and Feds: The Mafia and the American Labor Movement* (1st Edn. New York University Press, 2006)

Jacobson, M. *Terrorist Financing on the Internet* (June 2009) CTC Sentinel Vol. 2 Issue 6

Jacobson, M. *An Iranian Financial Intelligence Unit: Less than Meets the Eye* (Washington Institute for Near East Policy, 2 April 2007) <<http://www.washingtoninstitute.org/templateC05.php?CID=25>> accessed November 2016

Jarvie, N. *Control of Cybercrime – is an end to our privacy on the Internet a price worth paying? Part 1* (2003) 9(3) Computer and Telecommunications Law Review 76

Jarvie, N. *Control of Cybercrime – is an end to our privacy on the Internet a price worth paying? Part 2* (2003) 9(2) Computer and Telecommunications Law Review 110

Jarrett, H.M. & Bailie, M.W. (US Justice Department, Computer Crime and Intellectual Property Section) *Prosecuting Computer Crimes Manual, Chapter 1 “Computer Fraud and Abuse Act”* (Department of Justice, 14 January 2015) <<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>> accessed April 2018

Johnson, D.R. & Post, D.G. *Law and Borders: The Rise of Law in Cyberspace*, (1996) 48 Stanford Law Review 1367

Johnson, H.A. *The USA PATRIOT Act and Civil Liberties: A Closer Look* (USCAW Strategy Research Project, 15 March 2006) <<http://www.dtic.mil/dtic/tr/fulltext/u2/a449681.pdf>> accessed June 2018

Johnstons Archive *Deadliest Terrorist Attacks Worldwide* (July 2016) <<http://www.johnstonsarchive.net/terrorism/wrjp255i.html>> accessed November 2016

*Joint Action of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds from crime* (98/699/JHA) <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:333:0001:0003:EN:PDF>> accessed November 2016



Joint Committee on the Investigatory Powers Bill *Report of Session 2015-16* HL Paper 93/HC 651 (HMSO, 11 February 2016)  
<<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/9302.htm>> accessed November 2016

JUSTICE *Intercept Evidence: Lifting the Ban* (October 2006)  
<<http://www.justice.org.uk/data/files/resources/40/Intercept-Evidence-1-October-2006.pdf>> accessed November 2016

JUSTICE, *JUSTICE criticises government delays over intercept evidence* (10 December 2009) <<http://www.justice.org.uk/data/files/resources/62/10dec09-JUSTICE-criticises-government-delays-over-intercept-evidence.pdf>> accessed November 2016

JUSTICE *Freedom from Suspicion: Surveillance Reform for a Digital Age* (October 2011) <<http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf>> accessed November 2016

JUSTICE *Written Evidence to the Draft Investigatory Powers Bill Joint Committee* IPB0148 (HMSO, 17 December 2015)  
<[http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#\\_ftn21](http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26448.html#_ftn21)> accessed November 2016

Kadochnikov, A. *Regulatory Classification of the authorized Linden Dollar resellers* (epaylaw, 28 May 2013) <<http://www.epaylaw.com/2013/05/28/regulatory-status-of-linden-lab-and-authorized-linden-dollar-resellers-in-light-of-the-new-terms-of-service/>> accessed November 2016

Kampherstein, J.F. *Internet privacy legislation and the Carnivore system* (2000-2001) 19 Temp. Env't L & Tech. J 155

Keene, S.D. *Terrorism and the internet: a double-edged sword* (2011) Journal of Money Laundering Control, Vol. 14 Iss 4, 359 – 370

Kennedy, P. *Watching the clothes go round: Combating the effects of money laundering on economic development and international trade* (2003) 12 Current International Trade Law Journal 140

Kerry, J. (Sen.) & Brown, H. (Sen.) *The BCCI Affair: A Report to the Committee on Foreign Relations United States Senate* 102d Congress 2d Session Senate Print 102-140 (GPO, December 1992)

King Abdulaziz City Science and Technology Unit *ISU History*  
<<https://www.kacst.edu.sa/eng/ScientificServices/ISU/Pages/History.aspx>> accessed June 2018

Kirby, M. (Hon. Justice) *Information security – OECD Objectives* (1992) 3 Journal of Law and Inf. Sci. 25

Kiska, R. *Hate Speech: A Comparison between the European Court of Human Rights and the United States Supreme Court* (2012) 25 Regent University Law Review 107

Klug, F. Starmmer, K. & Keir, S. *The Three Pillars of Liberty: Political Rights and Freedoms in the United Kingdom* (1st Edn. Routledge, 1996)

Kruger, L. R42351 *CRS report to Congress Internet Governance and the Domain Name System: Issues for Congress* (18 November 2016)

<<https://fas.org/sgp/crs/misc/R42351.pdf>> accessed June 2018

Lander, S. *Review of the Suspicious Activity Reports Regime* (London: SOCA, March 2006)

Landman, S.I. *Funding Bin Laden's Avatar: A proposal for the regulation of virtual Hawalas* (2008-9) 35 William Mitchell Law Review 5159

LaRue, F. (UN Human Rights Council) *Report of the Special Rapporteur on the promotion and protection of the right of freedom of expression, Frank LaRue* (17 April 2013)

<[http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)> accessed November 2016

Law Commission *Criminal Law: Computer Misuse* Cm819 (HMSO, October 1989)

<<http://www.bailii.org/ew/other/EWLC/1989/186.pdf>> accessed November 2016

Lee, L. T. *USA PATRIOT Act and telecommunications: Privacy under attack* (2003) 29 Rutgers Computer & Technology Law Review 371

Levi, M. *Combating the Financing of Terrorism: A History and Assessment of the Control of Threat Finance* (2010) 50(4) British Journal of Criminology 650

Levitsky, M. *Review of US efforts to combat the International Narcotics Trade – Statement before the Subcommittee on International Security, International Organizations and Human Rights of the House Foreign Affairs Committee, Washington DC* (11 May 1993) 4 pt 1 Department of State Dispatch 386 (1993)

Levitt, M. *Stemming the Flow of Terrorist Financing: Practical and Conceptual Challenges* (2003) 27 Fletcher Forum of World Affairs 60

Levitt, M. A. *The Political Economy of Middle East Terrorism* (December 2002) Middle East Review of International Affairs, Volume 6 No. 4

<<http://meria.idc.ac.il/journal/2002/issue4/jv6n4a3.html>> accessed November 2016

Levitt, M. A. & Jacobson, M. *Combating the Financing of Transnational Threats* (Emirates Center for Strategic Studies and Research, 2008-2009)

<<http://washingtoninstitute.org/opedsPDFs/4a2d1476df4b3.pdf>>

Levitt, M. A. & Jacobson, M. *Follow the Money* (Los Angeles Times, 23 December 2008) <<http://washingtoninstitute.org/templateC06.php?CID=1201>> accessed November 2016

Levitt, M, A. & Jacobson, M. *Staying Solvent: Assessing al-Qaeda's Portfolio* (Washington Institute, November 2009) <<http://www.washingtoninstitute.org/policy-analysis/view/staying-solvent-assessing-al-qaedas-financial-portfolio>> accessed June 2018

Levitt, M. A. & Jacobson, M. *Targeting Terrorists' Financial Networks* (Jerusalem Post, 6 January 2009) <<http://washingtoninstitute.org/templateC06.php?CID=1205>> accessed November 2016

Lewis, J. A. *The Internet and Terrorism* (2005) 99 Am. Socy Intl. L Proc 112

Lieberman, J. I., (Chairman) & Collins, Susan M. (Ranking Member) *A Ticking Time Bomb: Counter-terrorism Lessons from the US Government's Failure to Prevent the Fort Hood Attack* 20510 (U.S. Senate Committee on Homeland Security and Governmental Affairs Washington D.C. February 2011) <[www.hsgac.senate.gov/public/files/Fort\\_Hood/FortHoodReport.pdf](http://www.hsgac.senate.gov/public/files/Fort_Hood/FortHoodReport.pdf)> accessed November 2016

Liberty *Liberty's response to Lord Carlile's review of the definition of terrorism* (June 2006) <<http://www.liberty-human-rights.org.uk/pdfs/policy06/response-to-carlile-review-of-terrorism-definition.pdf>> accessed November 2016

Liberty *Liberty's written evidence on the Investigatory Powers Bill* (March 2016) <<https://www.libertyhumanrights.org.uk/sites/default/files/Liberty%27s%20briefing%20on%20the%20Investigatory%20Powers%20Bill%20for%20Second%20Reading%20in%20the%20House%20of%20Commons.pdf>> accessed June 2018

Library of Congress *Congressional Record* 109<sup>th</sup> Congress, 2nd Session Issue: Vol. 152, No. 106 — Daily Edition, S8901-S8902 (3 August 2006) <<https://www.congress.gov/congressional-record/2006/08/03/senate-section/article/S8901-2?>> accessed November 2016

Library of Congress *Congressional Record* 107<sup>th</sup> Congress: V 148 Pt. 13 (September 20 2002 to October 1 2002)

Liu, E. C. R40138 *CRS Report to Congress Amendments to the Foreign Intelligence Surveillance Act (FISA) Extended United June 1 2015* (16 June 2011) <<https://fas.org/sgp/crs/intel/R40138.pdf>> accessed November 2016

Lloyd, C. *Written evidence submitted to the Public Bills Committee* IPB 35 (HMSO, 24 March 2016) <<http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB35.htm>> accessed November 2016

Lodgson, K.R. *Who knows you are reading this? The United States' domestic electronic surveillance in a post-9/11 world* (2008) *Journal of Law Technology & Policy* 409

Lombardi, C.B. *Islamic Law as a Source of Constitutional Law in Egypt: The Constitutionalization of the Sharia in Modern Arab States* (1998) 37(1) *Columbia Journal of Transnational Law* 81

Lord Carlile of Berriew *The Definition of Terrorism* Cm 7052 (Home Office, March 2007) <<https://www.gov.uk/government/publications/the-definition-of-terrorism-a-report-by-lord-carlile-of-berriew>> accessed April 2018

Lord Lloyd of Berwick *Inquiry into Legislation Against Terrorism* Volume 1 Cm 3420 (HMSO, 1996)

Lord Taylor of Holbeach *Hansard* HL Deb c421W (23 September 2013)

Lord Taylor of Holbeach *Hansard* HL Deb c1003 (12 December 2013)

Loundy, D. J. *E-law: Legal issues affecting computer information systems and systems operator liability* (1993) 3 Alb. L. J. Sci. & Tech. 79

Ludwig, T. P. *The erosion of privacy rights in the recent tide of terrorism* (2003-2004) 8 Computer Law Review & Technology Journal 131

Lundie, A. *Electronic Commerce – interception of communications – High Court confirms police powers to intercept e-mails* (2003) 9(1) Computer and Telecommunications Law Review N10

Lynch, J. *Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks* (2005) 20 Berkley Technology Law Journal 259

Madrinan, P. G. *Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act 2001* (2003) 64 University of Pittsburgh Law Review 783

Malcolm, J. *Multi-Stakeholder Governance and the Internet Governance Forum* (1<sup>st</sup> Edn. Terminus Press, 2008)

Mann, T. (ed.) *Australian Law Dictionary* (1<sup>st</sup> Edn. Oxford University Press, 2010)

Marès, F. *The Regulation of Investigatory Powers Act 2000: Overview of the case of R v Clifford Stanford (CA (Crim) 211, 1 February 2006) and the Offence of unlawfully intercepting communications on a private system* (2006) 22 Computer Law and Security Report 254

Marion, N. *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation* (2010) International Journal of Cyber Criminology Vol 4 Issue 1&2 700

Marlinspike, M. "A Saudi Arabia Telecom's Surveillance Pitch", *Thought Crime* (Blog, 13 May 2013) <<http://bit.ly/1011Ynw>> accessed November 2016

May, T. *Oral Statement* (Hansard, 8 June 2011) <<http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm110607/debtext/110607-0002.htm#11060740000001>> accessed November 2016

McAfee Internet Security *Net Losses: Estimating the Global Cost of Cybercrime: Economic impact of cybercrime II* (June 2014) <<https://www.csis.org/events/2014-mcafee-report-global-cost-cybercrime>> accessed April 2018

McCarthy, M. *USA PATRIOT Act* (2002) 39 Harvard Journal on Legislation 435, 435-436

- McClellan, J.L. (Sen.) *A bill to Outlaw the Mafia or Other Organized Crime syndicates* S. 2187, 89th Congress, (GPO, 24 June 1965)
- McNeal, G. S. *Cyber Embargo: Countering the Internet Jihad* (2008) 39 Case W. Res J Int'l Law 789
- Mei Leong, A. *Chasing Dirty Money: domestic and international measures against money laundering* (2007) 10(2) Journal of Money Laundering Control 140-156
- Mell, P. *Big Brother at the Door: Balancing National Security with Privacy under the USA PATRIOT Act* (2002) 80 Denver University Law Review 375
- Meyer, J. & Miller, G. *Secret U.S. Program Tracks Global Bank Transfers* (Blog, Common Dreams, 23 June 2006) <[www.commondreams.org/headlines06/0623-06.htm](http://www.commondreams.org/headlines06/0623-06.htm)> accessed November 2016
- Middle East North Africa Financial Action Task Force *Mutual Evaluation Report Saudi Arabia* (25 June 2010) <[www.menafatf.org/MER/MER\\_SaudiArabia\\_English.pdf](http://www.menafatf.org/MER/MER_SaudiArabia_English.pdf)> accessed November 2016
- Middle East North Africa Financial Action Task Force *Mutual Evaluation Report: 4th Follow-Up Report for Saudi Arabia* (17 June 2014) <[http://www.menafatf.org/sites/default/files/KSA\\_Exit\\_report\\_EN.pdf](http://www.menafatf.org/sites/default/files/KSA_Exit_report_EN.pdf)> accessed June 2018
- Mills, H. Skodbo, S. and Blyth, P. (Home Office) *Understanding organised crime: estimating the scale and the social and economic costs* (7 October 2013) <<https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs>> accessed November 2016
- Mills, J. *Internet Casinos: A sure bet for money laundering* (2001) 8(4) Journal of Financial Crime 365
- Montgomery, C. *Can Brandenburg v Ohio survive the Internet and the Age of Terrorism? The Secret Weakening of a Venerable Doctrine* (2009) 70 Ohio St. L.J. 141
- Moore, D. & Rid, T. *Cryptopolitik and the Darknet, Survival* (2016) Vol. 58 Iss. 1 <<http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>> accessed November 2016
- Morais, H. V. *Fighting International Crime and its financing: The importance of following a coherent global strategy based on the rule of law* (2005) 50 Villanova Law Review 583
- Morgan, S. *Cyber Crime Costs Projected To Reach \$2 Trillion by 2019* (Forbes, 17 January 2016) <<http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#118419f23bb0>> accessed November 2016.
- Mosaic Group *The Internet In Saudi Arabia* (1999) <[http://mosaic.unomaha.edu/SaudiArabia\\_1999.pdf](http://mosaic.unomaha.edu/SaudiArabia_1999.pdf)> accessed November 2016

- Mueller M., Mathiason, J. & Klein, H. *The Internet and Global Governance: Principals and Norms for a new regime* (2007) 13 *Global Governance* 237
- Mueller, R.S. *Statement Before the Senate Committee on Homeland Security and Governmental Affairs* (19 September 2012) <<http://www.fbi.gov/news/testimony/homeland-threats-and-agency-responses>> accessed November 2016
- Murray, A. *Information Technology Law: The Law and Society* (3rd Edn. Oxford University Press, 2016)
- Nieland, A.E. *National Security Letters and the amended PATRIOT Act* (2007) 92 *Cornell Law Review* 1201
- Nabbali, T. & Perry, M. *Going for the throat: Carnivore in an Echelon world* (2004) 20(2) *Computer Law & Security Review* 84
- National Audit Office *The regulatory effectiveness of the Charity Commission* HC 813 Session 2013-14 (4 December 2013) <<https://www.nao.org.uk/report/regulatory-effectiveness-charity-commission-2/>> accessed November 2016
- National Audit Office *Follow up on the Charity Commission* HC 908 Session 2014-15 (22 January 2015) <<https://www.nao.org.uk/report/follow-up-on-the-charity-commission/>> accessed November 2016
- National Crime Agency *Suspicious Activity Reports (SARs) Annual Report 2014* <<http://www.nationalcrimeagency.gov.uk/publications/464-2014-sars-annual-report>> accessed November 2016
- National Crime Agency *Suspicious Activity Reports (SARs) Annual Review 2015* <[www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015](http://www.nationalcrimeagency.gov.uk/publications/677-sars-annual-report-2015)>, accessed November 2016
- National Police Chiefs' Council *National channel referral figures* <<http://www.npcc.police.uk/FreedomofInformation/NationalChannelReferralFigures.aspx>> accessed November 2016
- National Union of Teachers *Prevent Strategy* (28 March 2016) <<https://www.teachers.org.uk/news-events/conference-2016/prevent-strategy>> accessed November 2016
- NATO A/66/359 *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General* (NATO Cooperative Cyber Defence Centre of Excellence, 14 September 2011) <[https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct\\_0.pdf](https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf)> accessed November 2016
- Netcraft *Web Server Survey* (March 2016) <<https://news.netcraft.com/archives/2016/03/18/march-2016-web-server-survey.html>> accessed November 2016
- Nettleton, E. & Watts, M. *Legal update: The Data Retention Directive* (2006) 14 *Database Marketing and Consumer Strategy Management* 74

Neumann, P. R. *Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s* (ICSR 26 January 2015)  
<<http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/>> accessed November 2016

Newland, L.S. *Money Laundering* (2008) 45 *American Criminal Law Review* 741

North, G. A. *Carnivore in Cyberspace: Extending the Electronic Communication Privacy Acts framework to Carnivore surveillance* (2002) 28 *Rutgers Computer Technology Law Journal* 155

Odoyo, S. *The Effects of US Counter-terrorist laws on International Business and Trade* (2010-2011) 38 *Syracuse Journal of International Law and Commerce* 257

Office for National Statistics *2011 Census: Key Statistics for England and Wales March 2011* (11 December 2012)  
<<http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/stb-2011-census-key-statistics-for-england-and-wales.html>> accessed November 2016

Office for National Statistics *Internet access – households and individuals: 2016* (4 August 2016)  
<<http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2016>> accessed November 2016

Office of the United Nations High Commissioner for Human Rights *Current Membership of the Human Rights Council*  
<<http://www.ohchr.org/EN/HRBodies/HRC/Pages/CurrentMembers.aspx>> accessed November 2016

OpenNet Initiative *Study on Saudi Arabia* <<http://opennet.net/studies/saudi>> accessed November 2016

OpenNet Initiative *Internet Filtering in Saudi Arabia* (2009)  
<[http://opennet.net/sites/opennet.net/files/ONI\\_SaudiArabia\\_2009.pdf](http://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf)> accessed November 2016

OpenNet Initiative *Saudi Arabia* (6 August 2009)  
<<https://opennet.net/research/profiles/saudi-arabia>> accessed November 2016

Open Rights Group *Sleepwalking into Censorship* (25 July 2013)  
<<https://www.openrightsgroup.org/blog/2013/sleepwalking-into-censorship>> accessed November 2016

Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD, 11 August 2016) <<https://www.eba.europa.eu/-/eba-publishes-an-opinion-on-the-commission-s-proposal-to-bring-virtual-currency-entities-in-the-scope-of-the-anti-money-laundering-directive>> accessed November 2016



Organisation for Economic Co-operation and Development OECD *OECD Guidelines for Consumer Protection in the context of e-commerce* (9 December 1999) <<http://www.oecd.org/dataoecd/18/13/34023235.pdf>> accessed November 2016

Ormand, S. *Pending U.S. Legislation to prohibit offshore Internet gambling may proliferate money laundering* (2004) 10 Law & Bus. Rev. Am. 447

Ormerod, D. & Williams, D. *The Fraud Act* (Legislative Comment) (2007) 1 Archbold News 6-9

Orr, A.E. *Marking Carnivore's territory: Rethinking Pen Registers on the Internet* (2001-2002) 8 Michigan Telecommunications & Technology Law Review 219

Outlaw.com *Revised UK interception of communications laws address EU privacy concerns* (26 January 2012) <<http://www.out-law.com/en/articles/2012/january-/revised-uk-interception-of-communications-laws-address-eu-privacy-concerns/>> accessed November 2016

Overseas Development Institute *UK humanitarian aid in the age of counterterrorism: perceptions and reality* (March 2015) <<https://www.odi.org/publications/9301-counter-terrorism-legislation-law-uk-muslim-ngos-charities-commission-humanitarian>> accessed November 2016

Paik, J.S. *RICO* (1988) 26 American Criminal Law Review 971

Parachini, J. *The World Trade Center Bombers* (1993) (Jonathan B. Tucker (ed.) *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons* (Cambridge MA: MIT Press, 2000))

Parliamentary Joint Committee on Human Rights *Counter-Terrorism Policy and Human Rights: Terrorism Bill and related matters* 3rd Report of Session 2005-2006 (HL Paper 75-I, HC 561-I, HMSO, 28 November 2005) <<http://www.publications.parliament.uk/pa/jt200506/jtselect/jtrights/75/75i.pdf>> accessed November 2016

Parliamentary Joint Committee on Counter Terrorism Policy and Human Rights *Counter Terrorism Policy and Human Rights (Seventeenth Report): Bringing Human Rights Back In* 16th Report of Session 2009-2010 (HL Paper 86, HC 111 HMSO, 25 March 2010) <<http://www.publications.parliament.uk/pa/jt200910/jtselect/jtrights/86/8602.htm>> accessed November 2016

Passas, N. *Setting Global CFT Standards: A Critique and Suggestions* (2006) Journal of Money Laundering Control, Vol. 9 Issue: 3, 281

Passas N., *Informal Value Transfer Systems and Criminal Organisations: A Study into so-called Underground Banking Networks* (14 December 1999) <[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1327756](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1327756)> accessed November 2016

Pathak, R. *The Obstacles to regulating the hawala: A cultural norm or a terrorist hotbed?* (2003) 27 Fordham International Law Journal 2007



Payfort *State of Payments 2016*

<<http://www.payfort.com/stateofpayments2016/#trends>> accessed November 2016

Payfort *Arab world could see US\$69 billion in online payment transactions per annum by 2020* (2 June 2016) <<http://www.payfort.com/press/arab-world-see-us69-billion-online-payment-transactions-per-annum-2020/>> accessed November 2016

Perkel, W. *Money Laundering and Terrorism: Informal Value Transfer Systems* (2004) 41 *American Criminal Law Review* 183

Pickles, E. *Written Statement: Integration Update HCWS154* (Hansard, 18 December 2014) <<http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2014-12-18/HCWS154/>> accessed November 2016

Pieth, M. *Financing of Terrorism: Follow the Money* (2002) 4 *European Journal of Law Reform* 365

Pieth, M. *Criminalizing the Financing of Terrorism* (2006) 4(5) *Journal of International Criminal Justice* 1074

Phillips, A. *Terrorist Financing Laws won't wash: It ain't money laundering* (2004) 23 *University of Queensland Law Journal* 81

Prados, A.B. & Blanchard, C.M. RL32499 *CRS Report to Congress – Saudi Arabia: Terrorist Financing Issues* (8 December 2004, updated 14 September 2007) <<https://fas.org/sgp/crs/terror/RL32499.pdf>> accessed June 2018

President George W. Bush *Joint Session of Congress Concerning the September 11, 2001 Terrorist Attacks on America* Congressional Record Volume 147, S9553-S9555 (GPO, 20 September 2001) <<http://www.gpo.gov/fdsys/pkg/CREC-2001-09-20/pdf/CREC-2001-09-20-pt1-PgS9553-4.pdf#page=1>> accessed November 2016

President Richard Nixon *American Presidency Project* (17 June 1971) <<http://www.presidency.ucsb.edu/ws/?pid=3048>> accessed April 2018

Privacy International *Statement of Grounds to the Investigatory Powers Tribunal* (9 July 2013) <[https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy\\_international\\_ipt\\_grounds.pdf](https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/privacy_international_ipt_grounds.pdf)> accessed November 2016

Privy Council *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications* Cmnd 283 (HMSO, 1957) <<http://www.fipr.org/rip/Birkett.htm>> accessed November 2016

Privy Council *Privy Council Review of Intercept as Evidence* Cm 7324 (HMSO, 30 January 2008) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228513/7324.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228513/7324.pdf)> accessed November 2016

Privy Council *Intercept as Evidence: A Report* Cm 7760 (HMSO, 10 December 2009) <[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/228715/7760.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228715/7760.pdf)> accessed April 2018

Privy Council *Intercept as Evidence* Cm 8989 (HMSO, 17 December 2014) <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/388898/InterceptAsEvidencePrint.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/388898/InterceptAsEvidencePrint.pdf)> accessed November 2016

Project ECOLEF *The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy* (February 2013) <[http://www2.econ.uu.nl/users/unger/ecolef\\_files/Final%20ECOLEF%20report%20\(digital%20version\).pdf](http://www2.econ.uu.nl/users/unger/ecolef_files/Final%20ECOLEF%20report%20(digital%20version).pdf)> accessed June 2018

Raab, S. *Five Families: The Rise, Decline, and Resurgence of America's Most Powerful Mafia Empires* (1<sup>st</sup> Edn. Chyrisalis Books Group, 2006)

Ramage, S. *2008 amendments of the Proceeds of Crime Act 2002 and other legislation that combats terrorist financing* (2008) Crim. Law 182, 1

Rensselaer, L. RL31658 *CRS Report to Congress Terrorist financing: The US and International Response* (6 December 2002) <[https://www.everycrsreport.com/files/20021206\\_RL31658\\_2009bbd56c90ec7f3a859cef3d688ad17afbf555.pdf](https://www.everycrsreport.com/files/20021206_RL31658_2009bbd56c90ec7f3a859cef3d688ad17afbf555.pdf)> accessed June 2018

Raphaeli, N. *Financing of Terrorism: Sources, Methods and Channels* (2003) 15(4) Terrorism and Political Violence 59

Ratner, A. *Warrantless wiretapping: The Bush Administration's failure to jam an elephant into a mousehole* (2009) 37 Hastings Const. L. Q. 167

Reidenberg, J.R. *Technology and Internet Jurisdiction* (2005) 153 U. Pa. L. Rev. 1951

Reid, A. S., & Ryder, N., *For Whose Eyes-Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000* (2001) I & CTL, 10 (2), 179-201

Reid, J. *Statement to Parliament* HC Deb, c31-32WS (Hansard, 10 December 2009)

Renieris, E. M. *Combating incitement to terrorism on the Internet: Comparative approaches in the United States and the United Kingdom and the need for an international solution* (2009) 11 Vand. J. Ent. & Tech. Law 673

Reporters without Borders *EU Court says Internet filtering violates freedom of information* (28 November 2011) <<http://en.rsfo.org/european-union-eu-court-says-internet-filtering-28-11-2011,41472.html>> accessed November 2016

Reporters without Borders *Saudi Arabia* <<https://rsfo.org/en/saudi-arabia>> accessed April 2018

- Rider, B. *Cyber-organised crime – the impact of information technology on organised crime* (2001) 8(4) *Journal of Financial Crime* 332
- Roach, K. *The 9/11 Effect: Comparative Counter-Terrorism* (1<sup>st</sup> Edn. Cambridge University Press, 2011)
- Rosette, D. *The Application of Real World Rules to Banks in Online Games and Virtual Worlds* (2008) 16 *U. Miami Bus. Law Rev.* 279
- Roth, J. Greenburg, D. & Wille, S. *National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission* (2004) <[https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)> accessed June 2018
- Ruff, K. *Scared to Donate: An Examination of the effects of designating Muslim charities as terrorist organizations on the First Amendment rights of Muslim donors* (2005) 9 *New York University Journal of Legislation and Public Policy* 447
- Ryder, N. *Danger Money* (2007) *New Law Journal* 157(7300) Sup (Charities Appeals Supplement) 6, 8
- Ryder, N. *Terror Funds – Charities and the Funding of Terrorism* (2007) *New Law Journal* 157 1305
- Ryder, N. *A False Sense of Security? An analysis of Legislative Approaches Towards to Prevention of Terrorist Finance in the United States and the United Kingdom* (2007) *J.B.L.* Nov 821
- Ryder, N & Türkşen, U. *Islamophobia or an important weapon? An analysis of the US financial war on terrorism* (2009) *Journal of Banking Regulation* 10(4) 307-320
- Ryder, N. *Financial Crime in the 21<sup>st</sup> Century: Law and Policy* (Edward Elgar, 2011)
- Ryder, N. *Banks in Defense of the Homeland: Nexus of Ethics and Suspicious Activity Reporting* (2013) *Contemporary Issues in Law* (Special Issue on Law, Ethics and Counter-Terrorism), 12(4), 311-347
- Ryder, N. *The Financial Crisis and White Collar Crime The Perfect Storm?* (Edward Elgar, 2014)
- Ryder, N. *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Routledge, 2015)
- Ryder, N. *Out with the old and ... in with the old? A critical review of the Financial War on Terrorism on the Islamic State of Iraq and Levant* (2016) *Studies in Conflict and Terrorism* (Special issue on 'Contemporary Issues, Innovation and Counter Terrorism')

Sathye, M. *Estimating the cost of compliance of AMLCTF for financial institutions in Australia* (2008) 15(4) *Journal of Financial Crime* 347

Saudi Arabia *The Kingdom of Saudi Arabia and Counterterrorism* (2016) <<https://28pagesdotorg.files.wordpress.com/2016/05/saudi-lobby-white-paper.pdf>> accessed November 2016

Saudi Arabia Communications and Information Technology Commission *About Us* <<http://www.citc.gov.sa/en/AboutUs/Pages/History.aspx>> accessed April 2018

Saudi Arabia Communications and Information Technology Commission *Introduction to Content Filtering, Communication and Information Technology Commission* <<http://www.citc.gov.sa/en/Pages/default.aspx>> accessed April 2018

Saudi Arabia Financial Intelligence Unit *Annual Report 2014* (Ministry of the Interior) <<https://www.moi.gov.sa/wps/portal/Home/sectors/safiu>> accessed November 2016

Saudi Arabia *General Authority for Zakat and Tax* <<https://www.gazt.gov.sa/en>> accessed April 2018

Saudi Arabian Ministry of Foreign Affairs *Counter-Terrorism International Conference* (26 October 2009) <<http://www.mofa.gov.sa/sites/mofaen/KingdomForeign-Policy/AntiTerrorism/Pages/AntiTerrorismConference35026.aspx>> accessed November 2016

Saudi Arabian Monetary Authority *Rules Governing Money Changing Business Issued by Decision of the Minister of Finance No. 1357 dated 01/05/1432H* <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p\\_SortBehavior=0&p\\_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p_SortBehavior=0&p_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed November 2016

Saudi Arabian Monetary Authority *Rules Governing Anti-Money Laundering & Combating Terrorist Financing Third Update, 2012* <[http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p\\_SortBehavior=0&p\\_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3](http://www.sama.gov.sa/en-US/Laws/Pages/BankingRulesAndRegulations.aspx?&p_SortBehavior=0&p_SAMAFFilePublishDate=20090412%2021%3a00%3a00&&PageFirstRow=1&View=077029df-1e4c-4158-b0e2-a959b0dddfc3)> accessed November 2016

Saudi Arabian Monetary Authority *The Kingdom of Saudi Arabia's Accession to Observer Member in FATF* (2 August 2015) <<http://www.sama.gov.sa/en-US/News/Pages/News08022015.aspx>> accessed November 2016

Saudi Telecom Company *Annual Report for STC 2009* <<https://www.stc.com.sa/wps/wcm/connect/english/stc/resources/9/6/964cbd96-c271-4dfe-9331-33b6d70d93a9/annual-report2009.pdf>> accessed April 2018

Saudi Telecom Company *Consolidated Financial Statements for the Year Ended 31 December 2015* <<https://www.stc.com.sa/wps/wcm/connect/english/stc/resources/8/c/8ccc40b1-82c2-4463-ad4d-a3e1e29851ee/2015.pdf>> accessed June 2018

Saudi-U.S. Trade Group *The Kingdom of Saudi Arabia and Counter-terrorism 2016 (Comprehensive Document Outlining Saudi Arabia's Counterterrorism Strategy, Successes Released)* (26 May 2016) <<http://sustg.com/comprehensive-document-outlining-saudi-arabias-counterterrorism-strategy-successes-released/>> accessed November 2016

Schott, P. *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2<sup>nd</sup> Edn. The International Bank for Reconstruction and Development, World Bank & International Monetary Fund, 2009)

Schwebel, S.M. *The Effect of Resolutions of the General Assembly on Customary International Law* (1979) 73 American Society of International Law Proceedings 301

Secretary of State for the Home Department, *Oral Statement to Parliament on the Publication of the Anderson Report* (11 June 2015) <<https://www.gov.uk/government/speeches/home-secretary-on-publication-of-the-anderson-report>> accessed November 2016

Select Committee on Home Affairs *First Report: Anti-Terrorism, Crime and Security Bill* (HMSO, 15 November 2001) <<http://www.publications.parliament.uk/pa/cm200102/cmselect/cmhaff/351/35103.htm>> accessed November 2016

Seymour, G. *Harry's Game* (1st Edn. Corgi, 1975)

Seymour, G. & Press, L. *The Global Diffusion of the Internet Project: An Initial Inductive Study* (1998) <<http://mosaic.unomaha.edu/GDI1998/7HSAUDI.PDF>> accessed November 2016

Sharp, J. M. RS21913 *CRS Report to Congress - Saudi Arabia: Reform and U.S. Policy* (13 October 2004) <<https://www.everycrsreport.com/reports/RS21913.html>> accessed November 2016

Shelton, D, ed. *Commitment and Compliance: The Role of Non-binding Norms in the International Legal System*. (Oxford University Press, 2000)

Shetterly, D. *Starving the terrorists of financing: How the US Treasury is fighting the war on terror* (2005-2006) 18 Regent University Law Review 327

Sidhu, D. S. *The chilling effects of Government surveillance programs on the use of the Internet by Muslim-Americans* (2007) 7 U. Md L.J. of Race, Religion, Gender & Class 375

Silke, A. *Contemporary terrorism studies: Issues in research: Critical Terrorism Studies: A New Research Agenda*, ed. Jackson, R., Breen Smyth, M., Gunning, J. (Routledge, 2009)

Simma, B, Khan, D.E., Nolte, G. & Paulus, A. (ed.) *The Charter of the United Nations: A Commentary* (3<sup>rd</sup> Edn. Oxford University Press, 2012)

Singh Guliani, N. *What's Next for Surveillance Reform After the USA Freedom Act* (ACLU Blog, 3 June 2015) <<https://www.aclu.org/blog/washington-markup/whats-next-surveillance-reform-after-usa-freedom-act>> accessed November 2016

Singh, M. & Singh, S. *Cyber Crime Convention and Transborder Criminality* (2007) 1 Masaryk U. J. L. & Tech. 53

Smith, M. RL31408 *CRS Report to Congress Internet Privacy: Overview and Legislation in the 109<sup>th</sup> Congress, 1<sup>st</sup> Session* (updated 26 January 2006) <<https://www.everycrsreport.com/reports/RL31408.html>> accessed June 2018

Smith, M. S., Seifert, J. W., McLoughlin, G. J. & Moteff, J. *CRS Report to Congress The Internet and the USA PATRIOT Act: Potential Implications for Electronic Security, Commerce and Government* (4 March 2002) <<https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-004.pdf>> accessed November 2016

Snowdon, P. & Lovegrove, S. *Money Laundering Regulations 2007* (2008) Compliance Officer Bulletin 54(Mar) 1

*Staff Statement No. 11 of the 9/11 Commission* <[http://govinfo.library.unt.edu/911/staff\\_statements/staff\\_statement\\_11.pdf](http://govinfo.library.unt.edu/911/staff_statements/staff_statement_11.pdf)> accessed November 2016

Stand for Peace *Camden Abu Dis Friendship Association* (24 September 2012) <<http://standforpeace.org.uk/camden-abu-dis-friendship-association/>> accessed November 2016

*Statement By J. Gilmore Childers, Esq. Orrick, Herrington & Sutcliffe LLP New York City, New York and Henry J. DePippo, Esq. Nixon Hargrave Devans & Doyle Rochester, New York, 6(b). Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information Hearing on "Foreign Terrorists in America: Five Years After the World Trade Center"* (24 February 1998) <[http://www.fas.org/irp/congress/1998\\_hr/s980224c.htm](http://www.fas.org/irp/congress/1998_hr/s980224c.htm)> accessed November 2016

Statista *Number of monthly active Facebook users worldwide as of 2nd quarter 2017 (in millions)* <<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>> accessed November 2017

Stevens, G.M. & Doyle, C. 98-326 *CRS Report to Congress Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (9 October 2012) <<https://fas.org/sgp/crs/intel/98-326.pdf>> accessed November 2016

Strafer, G.R. *Money Laundering: The Crime of the 90s* (1989-1990) 27 American Criminal Law Review 149

Stratford, J., Johnston, T. Brick Court Chambers *In the matter of surveillance: Advice* (22 January 2014) <[http://www.brickcourt.co.uk/news-attachments/APPG\\_Final\\_\(2\).pdf](http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf)> accessed June 2018



- Stratford, J. & Johnston, T. *The Snowden “revelations”: is GCHQ breaking the law?* (2014) E.H.R.L.R. 2014, 2 129
- Straub, J.P., *The Prevention of E-money Laundering: Tracking the elusive audit trail* (2001-2002) 25 Suffolk Transnat'l L. Rev. 515
- Stessens, G. *Money Laundering: A new International Law Enforcement Model* (Cambridge University Press, 2000)
- Stewart, D.P. *Internationalizing the War in Drugs: The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (1989-1990) 18 Denver Journal of International Law and Policy 388
- Sweeney, MJ. *Michael Adebolajo (Mujaahid Abu Hamza) and Michael Adebowale (Ismail Ibn Abdullah)* 26 February 2014 Sentencing remarks <<https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/adebolajo-adebowale-sentencing-remarks.pdf>> accessed June 2018
- Sutherland, E.H. *White Collar Crime* (New York: The Dryden Press, 1949)
- Sutter, G. *E-mail monitoring and interception 2001* (2001) 3 Electronic Business Law 2
- Techlaw Journal *Senate Ratifies Convention on Cybercrime* (3 August 2006) <<http://www.techlawjournal.com/topstories/2006/20060803b.asp>> accessed November 2016
- Testimony of Mr. Emmanuel Ogebe, Esq. On Behalf of the Jubilee Campaign On The Rising Global Threat of Boko Haram& US Policy Intransigence Before the Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations and the Subcommittee on Terrorism, Nonproliferation, and Trade, Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations*, (13 November 2013) <<https://oversight.house.gov/wp-content/uploads/2014/09/Mr.-Ogebe-Statement-Bio.pdf>> accessed November 2016
- The Holy Qur'an <<https://www.alislam.org/quran/>> accessed June 2018
- Theohary, C.A. & Rollins, J. R41674 CRS Report to Congress – *Terrorist Use of the Internet: Information Operations in Cyberspace* (8 March 2011) <<http://www.fas.org/sgp/crs/terror/R41674.pdf>> accessed November 2016
- Thomson Reuters *Technology in the fight against money laundering in the new digital currency age* (June 2013) <<https://www.int-comp.org/media/1047/technology-against-money-laundering.pdf>> accessed April 2018
- Thony, J.F. & Png Cheong, A. *FATF Special Recommendations and UN Resolutions on the Financing of Terrorism: A review of the status of implementation and legal challenges faced by countries* (2007) 14(2) Journal of Financial Crime 150
- Thornberry, T. *Written Question 40358* (Hansard, 27 June 2016) <<https://www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2016-06-13/40358>> accessed November 2016

Tibbetts, Lt Col P. S. *Terrorist Use of the Internet and Related Information Technology: A Monograph* School of Advanced Military Studies, Fort Leavenworth (2001-2002)

<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.859.2001&rep=rep1&type=pdf>> accessed June 2018

Tucker, P. C. *Digital Currency Doppelganger: Regulatory challenges or harbinger of the new economy?* (2009) 17 *Cardozo Journal of International & Computer Law* 589

Turner, S. *US Anti-Money Laundering Regulations: An economic approach to cyberlaundering* (2003-2004) 54 *Case W. Res. L. Rev.* 1389

UK Government Foreign Office Travel Advice *Timor Leste* <[www.gov.uk/foreign-travel-advice/timor-leste](http://www.gov.uk/foreign-travel-advice/timor-leste)> accessed 15 October 2016

UK National Counter Terrorism Security Office *Online radicalisation* (26 November 2015) <<https://www.gov.uk/government/publications/online-radicalisation/online-radicalisation>> accessed November 2016

United Nations *Terrorism*  
<<https://www.un.org/News/dh/infocus/terrorism/sg%20high-level%20panel%20report-terrorism.htm>> accessed November 2016

United Nations *UN Membership* <<http://www.un.org/en/members/index.shtml>> accessed November 2016

United Nations *Report of the Working Group on Internet Governance* (2005)  
<[www.wgig.org/docs/WGIGREPORT.pdf](http://www.wgig.org/docs/WGIGREPORT.pdf)> accessed November 2016

UN 10<sup>th</sup> Congress on the Prevention of Crime and Treatment of Offenders *Crime Fighting on the Net* (2000)  
<<https://www.un.org/press/en/2000/20000410.soccp216.doc.html>> accessed April 2018

United Nations Counter-Terrorism Implementation Task Force Working Group Compendium *Countering the Use of the Internet for Terrorist Purposes — Legal and Technical Aspects* (May 2011)  
<[http://www.un.org/en/terrorism/ctitf/pdfs/ctitf\\_interagency\\_wg\\_compendium\\_legal\\_technical\\_aspects\\_web.pdf](http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf)> accessed November 2016

United Nations Economic and Social Commission for Western Asia E/ESCWA/ICTD/2007/8 *Models for Cyber legislation in ESCWA Member Countries* (27 June 2007) <<https://www.unescwa.org/publications/models-cyber-legislation-escwa-member-countries>> accessed April 2018

United Nations Human Rights Council Twenty Ninth Session A/HRC/29/32 *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (Office of the United Nations High Commissioner for Human Rights, 22 May 2015)  
<[www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A.HRC.29.32\\_AEV.doc](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/.../A.HRC.29.32_AEV.doc)> accessed November 2016



United Nations Office on Drugs and Crime *Introduction to Money Laundering*  
<<http://www.unodc.org/unodc/en/money-laundering/introduction.html?ref=menuaside>> accessed November 2016

UN Office on Drugs and Crime *UN Manual on the Prevention and Control of Computer Related Crimes 1994*  
<[https://www.unodc.org/pdf/Manual\\_ComputerRelatedCrime.PDF](https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF)> accessed April 2018

United Nations Office on Drugs and Crime *Use of the Internet for terrorist purposes* (September 2012)  
<[http://www.unodc.org/documents/frontpage/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes.pdf](http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf)> accessed November 2016

United Nations Secretariat's Report A/CONF.121/22/Rev.1 *Seventh United Nations Congress on the Prevention of Crime and Treatment of Offenders* (UN Department of International Economic and Social Affairs, New York, 1986)  
<<http://www.asc41.com/7th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/030%20ACONF.121.22.Rev.1%20Seventh%20United%20Nations%20Congress%20on%20the%20Prevention%20of%20Crime%20and%20the%20Treatment%20of%20Offenders.pdf>> accessed November 2016

United Nations Secretariat's Working Paper *New Dimensions of Criminality and Crime Prevention in the Context of Development: Challenges for the Future* (Presented to the 7<sup>th</sup> United Nations Congress on the Prevention of Crime and Treatment of Offenders, Milan 26 August-6 September 1985)  
<<http://www.asc41.com/7th%20UN%20Congress%20on%20the%20Prevention%20of%20Crime/028%20ACONF.121.20%20New%20Dimensions%20of%20Criminality%20and%20Crime%20Prevention%20in%20the%20Context%20of%20Development.pdf>>;> accessed November 2016

United Nations Security Council *SECURITY COUNCIL CONDEMNS, 'IN STRONGEST TERMS', TERRORIST ATTACKS ON UNITED STATES* (12 September 2001) <<https://www.un.org/press/en/2001/SC7143.doc.htm>> accessed November 2016

United Nations Security Council S/2004/679 *First report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities* (25 August 2004) <<http://www.un.org/docs/sc/committees/1267/1267mg.htm>> accessed November 2016

United Nations Security Council *Narrative Summaries and Reasons for Listing QDe.071 AL-HARAMAIN ISLAMIC FOUNDATION (BOSNIA AND HERZEGOVINA)*  
<[https://www.un.org/sc/suborg/en/sanctions/1267/aq\\_sanctions\\_list/summaries/entity/al-haramain-islamic-foundation-\(bosnia-and-herzegovina\)](https://www.un.org/sc/suborg/en/sanctions/1267/aq_sanctions_list/summaries/entity/al-haramain-islamic-foundation-(bosnia-and-herzegovina))> accessed November 2016

United Nations Security Council *Consolidated United Nations Security Council Sanctions List* <<https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>> accessed November 2016

United Nations Treaty Collection *Economic Community of West African States Convention on Mutual Assistance in Criminal Matters* (1992) <<http://treaties.un.org/doc/Publication/UNTS/Volume%202329/Part/volume-2329-I-41737.pdf>> accessed November 2016

United Nations World Summit on the Information Society *Geneva Declaration of Principles* (2003) Document WSIS-03/GENEVA/DOC/4-E <[http://www.itu.int/dms\\_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf)> accessed November 2016

United Nations World Summit on the Information Society *Second Phase – Tunis Commitments* (2005) Document WSIS-05/TUNIS/DOC/7-E <<http://www.itu.int/wsis/docs2/tunis/off/7.pdf>> accessed November 2016

United Nations World Summit on the Information Society *Forum Outcome Document* (2016) <<https://www.itu.int/net4/wsis/forum/2016/Outcomes/#ft>> accessed November 2016

United States *National Strategy for Combating Terrorism* (14 February 2003) <[https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter\\_Terrorism\\_Strategy.pdf](https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf)> accessed June 2018

United States Attorney's Office Southern District of New York *Manhattan U.S. Attorney Announces \$731 Million Settlement Of Money Laundering And Forfeiture Complaint With Pokerstars And Full Tilt Poker* (31 July 2012) <<http://www.justice.gov/usao/nys/pressreleases/July12/pokersettlement.html>> accessed November 2016

United States Attorney's Office, Western District of Oklahoma *Fifty Seven Charged With Operating Illegal Online Sports Gaming Business* (10 April 2013) <[http://www.justice.gov/usao/okw/news/2013/2013\\_04\\_10.html](http://www.justice.gov/usao/okw/news/2013/2013_04_10.html)> accessed November 2016

United States Attorney's Office, Southern District of New York *Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A \$6 Billion Money Laundering Scheme* (28 May 2013) <<http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php>> accessed November 2016

United States Attorney's Office, District of Massachusetts *Judge Imposes Death Sentence for Boston Marathon Bomber* (24 June 2015) <<https://www.justice.gov/usao-ma/pr/judge-imposes-death-sentence-boston-marathon-bomber>> accessed November 2016

United States District Eastern District of Virginia *Notable cases United States v. Zacarias Moussaoui Criminal No. 01-455 A* <<http://www.vaed.uscourts.gov/notable-cases/moussaoui/exhibits/prosecution/OG00013.pdf>> accessed November 2016

*United States v. Colleen R. LaRose Indictment* Criminal No 10- (4 March 2010)  
<<http://jnsllp.com/wp-content/uploads/2010/03/indictment.pdf>> accessed November 2016

*United States v. Colleen R. LaRose Government's Change of Plea Memorandum* Criminal No. 10-123-01 (28 January 2011) <<http://www.jnsllp.com/wp-content/uploads/2011/02/plea-memo-larose.pdf>> accessed November 2016

*United States v. Jamie Paulin Ramirez Government's Change of Plea Memorandum* Criminal No. 10-123-02 (4 March 2011) <<http://jnsllp.com/wp-content/uploads/2011/03/plea-memo-paulin-ramirez.pdf>> accessed November 2016

US Census Bureau *Census* <<http://www.census.gov/main/www/popclock.html>> accessed 16 February 2012

US Department of Justice *Online Fraud* <<https://www.justice.gov/criminal-fraud>> accessed April 2018

US Department of Justice *Meeting of Justice and Interior Ministers of Eight Communiqué* (10 December 1997) <<https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf>> accessed April 2018

US Department of Justice *Statement by Attorney General Janet Reno on the Meeting of Justice and Interior Ministers of Eight* (10 December 1997)  
<<http://www.justice.gov/opa/pr/1997/December97/518cr.html>> accessed November 2016

US Department of Justice *G-8 Lyon Subgroup on Hi-Tech Crime: Communiqué* (10 December 2007)  
<<https://www.justice.gov/sites/default/files/ag/legacy/2004/06/08/97Communique.pdf>> accessed April 2018

US Department of Justice *Letter to Nancy Pelosi, Speaker at the House of Representatives from the Attorney General, Michael Mukasey and the Director of National Intelligence, J.M. McConnell* (19 June 2008)  
<<http://www.justice.gov/archive/ll/docs/ag-dni-fisa-letter061908.pdf>> accessed November 2016

US Department of Justice *Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges* (21 July 2008)  
<<http://www.usdoj.gov/opa/pr/2008/July/08-crm-635.html>> accessed November 2016

US Department of Justice *Letter from Ronald Welch, Assistant Attorney General, to Sen. Patrick Leahy and Sen. Jeff Sessions* (26 March 2010)  
<<http://www.justice.gov/cjs/docs/terrorism-crimes-letter.pdf>> accessed November 2016

US Department of Justice *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (Office of the Inspector General, March 2008), 114  
<<http://www.justice.gov/oig/special/s0803b/final.pdf>> accessed November 2016

US Department of Justice *FISA report 2011* (30 April 2012)  
<<http://www.fas.org/irp/agency/doj/fisa/2011rept.pdf>> accessed November 2016

US Department of Justice *Maryland Man Pleads Guilty to Conspiracy to Provide Material Support to Terrorists* (4 May 2012)  
<<http://www.justice.gov/opa/pr/2012/May/12-nsd-579.html>> accessed November 2016

US Department of Justice *Letters from Peter J Kadzik, Principal Deputy Assistant Attorney General, to Harry Reid, Majority Leader, US Senate, Nancy Pelosi, Minority Leader, US House of Representatives, Mitch McConnell, Minority Leader, US Senate, Eric Cantor, Majority Leader, US House of Representatives, John Boehner, Speaker, US House of Representatives, Joseph R. Biden Jr, President, US Senate, and Patrick J. Leahy, Chairman, Committee on the Judiciary* (30 April 2013) <[http://www.justice.gov/nsd/foia/foia\\_library/2012fisa-ltr.pdf](http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf)> accessed November 2016

US Department of Justice *Computer Crime and Intellectual Property Section*  
<<https://www.justice.gov/criminal-ccips>> accessed April 2018

US Department of State *Mutual Legal Assistance Treaty between the United States of America and the European Union*, (25 June 2003, Entry into force 1 February 2010) <<https://www.state.gov/documents/organization/180815.pdf>> accessed April 2018

US Department of State *Saudi Arabia 2015 Human Rights*  
<<http://www.state.gov/documents/organization/253157.pdf>> accessed November 2016

US Department of State *Country Reports on Terrorism 2015 Chapter 2. Country Reports: Middle East and North Africa Overview*  
<<http://www.state.gov/j/ct/rls/crt/2015/257517.htm>> accessed November 2016

US Department of State *Fact Sheet: Taking Stock of the Counter-ISIL Finance Group's Achievements in its First Year* (12 April 2016)  
<<http://www.state.gov/e/eb/rls/othr/2016/255765.htm>> accessed November 2016

US Department of State *The Treaty of Alliance with France; US Department of State U.S. Relations with France* (21 July 2016)  
<<http://www.state.gov/r/pa/ei/bgn/3842.htm>> accessed November 2016

US Department of State *State Sponsors of Terrorism*  
<<http://www.state.gov/j/ct/list/c14151.htm>> accessed November 2016

US Department of State Bureau of Counterterrorism *Foreign Terrorist Organizations* <<https://www.state.gov/j/ct/rls/other/des/123085.htm>> accessed April 2018

US Department of the Treasury *Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S. Based Charities* 2002 (updated in 2006)  
<[http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines\\_charities.pdf](http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines_charities.pdf)> accessed November 2016

US Department of the Treasury & FinCEN *Feasibility Study of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act* (October 2006) <[www.fincen.gov/news\\_room/rp/files/CBFTFS\\_Complete.pdf](http://www.fincen.gov/news_room/rp/files/CBFTFS_Complete.pdf)> accessed November 2016

US Department of the Treasury *U.S. National Money Laundering Strategy 2007* <<https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/nmls.pdf>> accessed April 2018

US Department of the Treasury *Best Practice Guidelines for charities* (2010) <[https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines\\_charities.pdf](https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/guidelines_charities.pdf)> accessed April 2018  
US Department of the Treasury *Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311* (28 May 2013) <<http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx>> accessed November 2016

US Department of The Treasury *Specially Designated Nationals List* (Office of Foreign Assets Control) <<https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>> accessed November 2016

US Department of the Treasury *List of Designated Charities under Executive Order 13,224* <<http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/designationsum-.pdf>> accessed November 2016

US Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations *HSBC Exposed U.S. Financial System to Money Laundering, Drug, Terrorist Financing Risks* (16 July 2012) <<https://www.hsgac.senate.gov/subcommittees/investigations/media/hsbc-exposed-us-finacial-system-to-money-laundering-drug-terrorist-financing-risks>> accessed November 2016

US Homeland Security & Governmental Affairs Permanent Subcommittee on Investigations *U.S. Vulnerabilities to Money Laundering, Drugs and Terrorist Financing: HSBC Case History* (17 July 2012) <<http://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history>> accessed November 2016

US House of Representatives *Expressing the sense of Congress regarding actions to preserve and advance the multistakeholder governance model under which the Internet has thrived* 112th Congress, H.Con.Res.127 (2 August 2012) <<https://www.congress.gov/bill/112th-congress/house-concurrent-resolution/127/text>> accessed November 2016

US House of Representatives Committee on Homeland Security *Written Statement of Andrew R. Cochran For the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing U.S. House Committee on Homeland Security* (31 March 2009) <<https://www.coursehero.com/file/10024718/Counterterrorism-blog/>> accessed November 2016

US House of Representatives Financial Services Committee *FBI Confirms Online Gambling Opens Door To Fraud, Money Laundering; Age Verification Software Ineffective* (3 December 2009) <<http://financialservices.house.gov/News/DocumentSingle.aspx?DocumentID=227740>> accessed November 2016

US House of Representatives Financial Services Committee *Too Big to Jail: Inside the Obama Justice Department's Decision not to hold Wall Street Accountable* (11 July 2016) <[financialservices.house.gov/uploadedfiles/07072016\\_oi\\_tbtj\\_sr.pdf](http://financialservices.house.gov/uploadedfiles/07072016_oi_tbtj_sr.pdf)> accessed November 2016

US Securities and Exchange Commission *Ponzi Schemes* <<https://www.sec.gov/answers/ponzi.htm>> accessed November 2016

US Senate *PATRIOT Act Reauthorization s.1038 Legislative Bulletin* (Democratic Policy and Communications Center, 23 May 2011) <<http://dpc.senate.gov/docs/lb-112-1-14.pdf>> accessed November 2016

US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence *Joint Inquiry into Intelligence Community activities before and after the terrorist attacks of September 11, 2001* (December 2002) <[https://fas.org/irp/congress/2002\\_rpt/911rept.pdf](https://fas.org/irp/congress/2002_rpt/911rept.pdf)> accessed June 2018

US Senate Select Committee on Intelligence *Director of the NSA, General Alexander's remarks to the Senate Intelligence Committee* (18 June 2013) <[https://fas.org/irp/congress/2013\\_hr/disclosure.pdf](https://fas.org/irp/congress/2013_hr/disclosure.pdf)> accessed June 2018

Vallance, P. *UK & US National Perspectives: Money Laundering and Asset Forfeiture – an Update* (1993) 19 Commonwealth Law Bulletin 1852

VanWasshnova, M.R. *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* (2006-2008) 39 Case W. Res. Journal of International Law 827

Vatis, M. A. *The Council of Europe Convention on Cybercrime* (2010) Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy <<http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf>> accessed April 2018

Vervaele, J.A.E. *The Anti-terrorist legislation in the US: Inter Arma Silent Leges* (2005) 13(2) European Journal of Crime, Criminal Law and Criminal Justice 201

Vervaele, J.A.E. *The Anti-Terrorist Legislation in the US: Criminal Law for the Enemies?* (2006) 8 European Journal of Law Reform 137

Vilasau, M. *Traffic Data Retention v Data Protection: the new European Framework* (2007) Computer Technology Law Review 13(2) 52

Villa, J.K. *A Critical View of Bank Secrecy Act Enforcement and the Money Laundering Statutes* (1987-1988) 37 Catholic University Law Review 489



Wall, D. *The Internet as a conduit for criminal activity* (2005) (Pattavina, A. (ed) *Information Technology and the Criminal Justice System* Thousand Oaks CA: Sage. Chapter revised March 2010)

Walter, C. *Defining Terrorism in National and International Law* (2004)  
<[https://www.unodc.org/tldb/bibliography/Biblio\\_Terr\\_Def\\_Walter\\_2003.pdf](https://www.unodc.org/tldb/bibliography/Biblio_Terr_Def_Walter_2003.pdf)> accessed November 2016

Ward, C.A. *Building Capacity to Combat Terrorism: The Role of the United Nations Security Council* (2003) 8(2) *Journal of Conflict & Security Law* 289

Weaver, S.J. *Modern Day Money Laundering: Does the solution exist in the expansive system of monitoring and record-keeping regulation?* (2005) 24 *Annual Review of Banking and Finance Law* 443

Weber, A.M. *The Council of Europe's Convention on Cybercrime* (2003) 18 *Berkley Technology Law Journal* 425

Weinberg, J. *Everyone's a Winner: Regulating, not prohibiting, Internet gambling* (2005-2007) 35 *Southwest University Law Review* 293

Weimann, G. *www.terror.net – How Modern Terrorism Uses the Internet* (March 2004) *Special Report* 116 *United States Institute of Peace* 10

Weiss, M.A. RL32539 *CRS Report for Congress - Terrorist Financing: Current Efforts and Policy Issues for Congress* (20 August 2004)  
<<http://www.au.af.mil/au/awc/awcgate/crs/rl32539.pdf>> accessed June 2018

Wendell, O. *The Path of the Law* (1897) 10(8) *Harvard Law Review* 457

Westby, J.R. *Countering Terrorism with Cyber-Security* (2006-7) 47 *Jurimetrics* 297

Westmacott, P. *Big Brother never forgets – the data retention provisions of the Anti-terrorism, Crime and Security Act 2001* (2002) 18(3) *Computer Law & Security Review* 205

Wheatley, J.A. *Ancient Banking, Modern Crimes: How Hawala secretly transfers the finances of criminals and thwarts existing laws* (2005) 26 *University of Pennsylvania Journal of International Economic Law* 347

Whitehouse Archives *President Freezes Terrorists' Assets* (24 September 2001)  
<<https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>> accessed November 2016

Whitehouse Archives *Safeguarding America: President Bush signs PATRIOT Act Reauthorisation* (9 March 2006) <<https://www.justice.gov/archive/opa/docs/patriotact03-09-06.pdf>> accessed April 2018

Whitehouse Archives *Cyberspace Policy Review* (June 2011)  
<<https://obamawhitehouse.archives.gov/cyberreview/documents/>> accessed April 2018

Whitehouse Press Office *FACT SHEET: U.S. Contributions to NATO Capabilities* (8 July 2016) <<https://www.whitehouse.gov/the-press-office/2016/07/08/fact-sheet-us-contributions-nato-capabilities>> accessed November 2016

Whitley, E.A. & Hosein, I. *Policy Discourse and data retention: the technology politics of surveillance in the United Kingdom* (2005) 29 Telecommunications Policy 357

Whitton, M. *Progression and Technological Advancement of Terrorist Financing: Are Current Laws Adequate?* (December 2005)  
<[http://www.ibrarian.net/navon/paper/Progression and Technological Advancement of Terr.pdf?paperid=5381481](http://www.ibrarian.net/navon/paper/Progression_and_Technological_Advancement_of_Terr.pdf?paperid=5381481)> accessed November 2016

Wilcke, C. *Human Rights and Saudi Arabia's Counterterrorism Response; Religious Counselling, Indefinite Detention, and Flawed Trials* (Human Rights Watch, 10 August 2009) <<https://www.hrw.org/report/2009/08/10/human-rights-and-saudi-arabia-counterterrorism-response/religious-counseling>> accessed June 2018

Williams, A. F. *Prosecuting Website Development under the Material Support to terrorism statutes: Time to fix what's broken* (2007-8) 11 N.Y.U. J. Legis & Pub Pol'y 365

Winner, L. *Autonomous Technology: Technics out-of-control as a Theme in Political Thought* (1<sup>st</sup> Edn. MIT Press, 1977)

Wright, E.E. *Right to privacy in electronic communications: Current Fourth Amendment and statutory protection in the wake of Warshak v United States* (2007-2008) 3 I.S.J.L.P. 531

Wyden, R. (Sen.) *Law and Policy Efforts to Balance Security, Privacy and Civil Liberties in Post-9/11 America* (2006) 17 Stan. L. and Pol'y Rev 331

Yeates, J. *CALEA and RIPA: The US and the UK responses to wiretapping in an increasingly wireless world* (2001-2002) 12 Alb. L. J. Sci. & Tech 125

### **News Commentary:**

#### **ABC News**

ABC News (31 July 2012) *PokerStars in \$731M Money Laundering Settlement*  
<<http://abcnews.go.com/blogs/business/2012/07/pokerstars-in-731m-money-laundering-settlement/>> accessed November 2016

#### **Al Jazeera**



Al Jazeera (23 November 2014) *Saudi Arabia 'intensifies Twitter crackdown'*  
<<http://www.aljazeera.com/news/middleeast/2014/11/saudi-arabia-intensifies-twitter-crackdown-2014112363955848622.html>> accessed November 2016

York, J.C. (Al Jazeera, 29 March 2011) *The booming business of Internet censorship*  
<<http://www.aljazeera.com/indepth/opinion/2011/03/2011329113450125509.html>> accessed November 2016

## **BBC News**

BBC News (4 March 2001) *The IRA Campaigns in England*  
<<http://news.bbc.co.uk/1/hi/uk/1201738.stm>> accessed November 2016

BBC News (31 December 2003) *Web's Inventor Gets Knighthood*  
<<http://news.bbc.co.uk/1/hi/technology/3357073.stm>> accessed November 2016

BBC News (25 May 2007) *Betonsports admits racketeering*  
<<http://news.bbc.co.uk/1/hi/business/6689813.stm>> accessed November 2016

BBC News (28 April 2009) *Trio cleared over 7/7 attacks*  
<<http://news.bbc.co.uk/1/hi/uk/7507842.stm>> accessed November 2016

BBC News (11 February 2010) *European Swift bank data ban angers U.S.*  
<<http://news.bbc.co.uk/1/hi/world/europe/8510471.stm>> accessed November 2016

BBC News (21 September 2010) *Extremist websites skyrocketing, says Interpol*  
<<http://www.bbc.co.uk/news/world-europe-11382124>> accessed November 2016

BBC News (20 October 2011) *Two charged over 'Jihad Jane' terror plot*  
<<http://www.bbc.co.uk/news/world-us-canada-15396382>> accessed November 2016

BBC News (26 March 2012) *Coutts fined for failings in money laundering controls*  
<<http://www.bbc.co.uk/news/business-17512140>> accessed November 2016

BBC News (20 June 2012) *Mohammed Abdul Hasnath jailed for 14 months over terror charges* <<http://www.bbc.co.uk/news/uk-england-london-18528573>> accessed November 2016

BBC News (6 December 2012) *Al-Qaeda material bride Ruksana Begum jailed*  
<<http://www.bbc.co.uk/news/uk-england-london-20629275>> accessed November 2016

BBC News (11 December 2012) *HSBC to pay \$1.9bn in US money laundering penalties* <<http://www.bbc.co.uk/news/business-20673466>> accessed November 2016

BBC News (27 May 2013) *Liberty Reserve digital money service forced offline*  
<<http://www.bbc.co.uk/news/technology-22680297>> accessed November 2016

BBC News (13 June 2013) *NSA Chief says data disrupted 'dozens' of plots*  
<<http://www.bbc.co.uk/news/world-us-canada-22883078>> accessed November 2016

BBC News (18 November 2013) *Google and Microsoft agree steps to block abuse images* <<http://www.bbc.co.uk/news/uk-24980765>> accessed November 2016

BBC News (13 January 2014) *Men told to repay Birmingham terror plot cash* <<http://www.bbc.co.uk/news/uk-england-birmingham-25703118>> accessed November 2016

BBC News (20 January 2015) *Sky to block pornography by default to protect children* <<http://www.bbc.co.uk/news/technology-30896813>> accessed November 2016

BBC News (3 December 2015) *Islamic State: Where key countries stand* <<http://www.bbc.co.uk/news/world-middle-east-29074514>> accessed November 2016

BBC News (11 February 2016) *Manchester student guilty of terror offences* <<http://www.bbc.co.uk/news/uk-england-manchester-35549985>> accessed November 2016

BBC News (11 March 2016) *Radicalisation fear over cucumber drawing by boy, 4* <<http://www.bbc.co.uk/news/uk-england-beds-bucks-herts-35783659>> accessed November 2016

BBC News (9 April 2016) *Brussels explosions: What we know about airport and metro attacks* <<http://www.bbc.co.uk/news/world-europe-35869985>> accessed November 2016

BBC News (20 May 2016) *Paris attacks: Salah Abdeslam stays silent in French court* <<http://www.bbc.co.uk/news/world-europe-36340739>> accessed November 2016

BBC News (9 June 2016) *Paris attacks: Mohamed Abrini to be extradited to France* <<http://www.bbc.co.uk/news/world-europe-36492309>> accessed November 2016

BBC News (22 July 2016) *Nice lorry attack: Five suspected accomplices charged* <<http://www.bbc.co.uk/news/world-europe-36859312>> accessed November 2016

BBC News (19 August 2016) *Nice attack: What we know about the Bastille Day killings* <<http://www.bbc.co.uk/news/world-europe-36801671>> accessed November 2016

BBC News (19 October 2016) *Saudi blogger Raif Badawi 'faces new round of lashes'* <<http://www.bbc.co.uk/news/world-middle-east-37703312>> accessed November 2016

BBC News (17 November 2016) *'Jihadi Jack' parents to stand trial on suspicion of funding terrorism* <<http://www.bbc.co.uk/news/uk-england-oxfordshire-38015900>> accessed November 2016

Casciani, D. (BBC News, 19 July 2015) *Cyber-jihadist Babar Ahmad released* <<http://www.bbc.co.uk/news/uk-33585959>> accessed November 2016

Irshaid, F. (BBC News, 19 June 2014) *How Isis is spreading its message online* <<http://www.bbc.co.uk/news/world-middle-east-27912569>> accessed November 2016

Kotecha, S. (BBC News, 21 January 2016) *More than 400 children under 10 referred for 'deradicalisation'* <<http://www.bbc.co.uk/news/uk-35360375>> accessed November 2016

Usher, S. (BBC News, 7 December 2010) *Saudi royal succession: Professor detained over article* <<http://www.bbc.co.uk/news/world-middle-east-11936421>> accessed November 2016

Ward, M. (BBC News, 31 January 2014) *UK Government tackles wrongly-blocked websites* <<http://www.bbc.co.uk/news/technology-25962555>> accessed November 2016

## **Bloomberg**

Harris, A. (Bloomberg, 10 April 2013) *Legendz Online Gambling Probe Produces Charges Against 34* <<http://www.bloomberg.com/news/2013-04-10/legendz-online-gambling-probe-produces-charges-against-34.html>> accessed November 2016

## **CBS News**

CBS New York (6 October 2012) *Five Terrorism Suspects Appear In Federal Courts In Manhattan And New Haven* <<http://newyork.cbslocal.com/2012/10/06/five-terrorism-suspects-appear-in-federal-courts-in-manhattan-and-new-haven/>> accessed November 2016

Kerr, D. (CBS News, 31 May 2013) *Feds don't plan to take down Bitcoin or other currencies* (31 May 2013) <[http://www.cbsnews.com/8301-205\\_162-57587059/feds-dont-plan-to-take-down-bitcoin-or-other-currencies/](http://www.cbsnews.com/8301-205_162-57587059/feds-dont-plan-to-take-down-bitcoin-or-other-currencies/)> accessed November 2016

## **CNN**

CNN (7 February 2001) *Larry King Live: John Ashcroft Discusses His New Job as Attorney General* transcript <<http://edition.cnn.com/TRANSCRIPTS/0102/07/lkl.00.html>> accessed November 2016

CNN (9 November 2003) *Saudi official blames Riyadh attacks on al Qaeda* <<http://edition.cnn.com/2003/US/11/08/saudi.explosion/>> accessed November 2016

Castillo, M., Haddad, M., Martinez, M. & Almasry, S. (CNN, 16 November 2016) *Paris suicide bomber identified; ISIS claims responsibility for 129 dead* <<http://edition.cnn.com/2015/11/14/world/paris-attacks/>> accessed November 2016

Jamjoun, M. (CNN, 8 May 2014) *Saudi activist sentenced to 10 years, 1,000 lashes for insulting Islam* <<http://edition.cnn.com/2014/05/07/world/meast/saudi-activist-sentenced/>> accessed November 2016

Lister, T. & Cruickshank, P. (CNN, 11 June 2013) *Intercepted communications called critical in terror investigations* <<http://edition.cnn.com/2013/06/11/us/nsa-data-gathering-impact>> accessed November 2016

Mears, B. (CNN, 21 January 2009) *Justices refuse to reconsider law restricting Internet porn* <<http://edition.cnn.com/2009/TECH/01/21/supreme.court.reject/>> accessed November 2016

### **Financial Times**

Arnold, M. (Financial Times, 4 March 2015) *Finance Denied to Charities in Conflict Zones, Report Finds* <<https://www.ft.com/content/540bdd9e-c299-11e4-a59c-00144feab7de>> accessed November 2016

Khalaf, R. & Jones, S. (Financial Times, 17 June 2014) *Selling terror: how Isis details its brutality* <<https://www.ft.com/content/69e70954-f639-11e3-a038-00144feabdc0>> accessed November 2016

### **International Business Times**

Akinyemi, A. (International Business Times, 28 September 2014) *White Widow Samantha Lewthwaite 'Training Isis Suicide Bombers in Syria'* <<http://www.ibtimes.co.uk/white-widow-samantha-lewthwaite-training-isis-suicide-bombers-syria-1467558>> accessed November 2016

Neal, R. (International Business Times, 26 November 2013) *UK Internet Censorship: David Cameron Says Government Will Block 'Extremist' Websites* <<http://www.ibtimes.com/>> accessed November 2016

### **LA Times**

Meyer, J. (Los Angeles Times, 15 January 2006) *U.S. Faults Saudi Efforts on Terrorism* <<http://articles.latimes.com/2006/jan/15/world/fg-saudi15>> accessed November 2016

### **NBC**

NBC (Transcript, 8 June 2013) *Director James R. Clapper interview with Andrea Mitchell, NBC News Chief Foreign Affairs Correspondent* <<http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell?tmpl=component&format=pdf>> accessed November 2016

Dedman, B. & Schoen, J. (NBC News, 30 April 2013) *Adding up the financial costs of the Boston bombings* <<http://usnews.nbcnews.com/news/2013/04/30/17975443-adding-up-the-financial-costs-of-the-boston-bombings>> accessed November 2016

## **New York Times**

Cain, C. (New York Times Daily Report, 14 June 2013) *Secret Court Ruling in 2008 Put Technology Companies in Bind* <<http://bits.blogs.nytimes.com/2013/06/14/daily-report-secret-court-ruling-in-2008-put-technology-companies-in-bind/?ref=foreign-intelligence-surveillance-act-fisa>> accessed November 2016

Gilpeth, K. (New York Times, 18 December 2001) *Republic New York Pleads Guilty to Securities Fraud* <<http://www.nytimes.com/2001/12/18/business/republic-new-york-pleads-guilty-to-securities-fraud.html>> accessed November 2016

Santora, M., Rashbaum, W.K. & Perlroth, M. (New York Times, 28 May 2013) *Online Currency Exchange Accused of Laundering \$6 billion* <<http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=2&r=0>> accessed November 2016

Schmitt, E., Sanger, D.E. & Savage, S. (New York Times, 7 June 2013) *Administration says mining of data is crucial to fight terror* <<http://www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?hpw>> accessed November 2016

## **News.com.au**

Wilson, L. (News.com.au., 28 March 2015) *The rapid evolution of the ISIS death cult* <<http://www.news.com.au/world/middle-east/the-rapid-evolution-of-the-isis-death-cult/news-story/74f78cd251d7d700cfb9645c5b119f3d>> accessed 16 October 2016

## **Reuters**

Reuters/CNBC (31 May 2013) *Digital Currency Firms Rush to Adopt Regulations* <<http://www.cnn.com/id/100781308>> accessed November 2016

Reuters (18 April 2016) *Islamic State's income drops 30 per cent on lower oil, tax revenue* <<http://www.reuters.com/article/us-mideast-crisis-iraq-syria-islamic-state/USKCN0XF0D5>> accessed November 2016

Vicini, J. (Reuters, 21 June 2010) *The Supreme Court on Monday upheld a law that bars Americans from providing support to foreign terrorist groups, rejecting arguments that it violated constitutional rights of free speech and association* <<http://www.reuters.com/article/2010/06/21/us-usa-security-court-idUSTRE65K4B420100621>> accessed November 2016

## **The Guardian**

Agence France-Presse (The Guardian, 1 February 2015) *Saudi Arabia frees associate of imprisoned blogger Raif Badawi* <<https://www.theguardian.com/world/2015/feb/01/saudi-arabia-frees-raif-badawi-associate>> accessed November 2016

Black, I. (The Guardian, 24 May 2013) *Inspire magazine: the self-help manual for al-Qaida terrorists* <<https://www.theguardian.com/world/shortcuts/2013/may/24/inspire-magazine-self-help-manual-al-qaida-terrorists>> accessed November 2016

Black, I. (The Guardian Newspaper, 10 June 2013) *NSA Spying Scandal: What we have learned* <<http://www.guardian.co.uk/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned>> accessed November 2016

Borger, J. (The Guardian, 5 August 2002) *Bush held up plan to hit Bin Laden* <<https://www.theguardian.com/world/2002/aug/05/afghanistan.usa1>> accessed November 2016

Bowcott, O. (The Guardian, 7 July 2016) *Fifteen secret warrants in force granting bulk data collection in UK* <<https://www.theguardian.com/law/2016/jul/07/fifteen-secret-warrants-in-force-granting-bulk-data-collection-in-the-uk>> accessed November 2016

Bowers, S. (The Guardian, 9 April 2013) *Ray Bitar, Full Tilt Founder, strikes deal with US prosecutors* <<http://www.guardian.co.uk/uk/2013/apr/09/ray-bitar-full-tilt-poker-pleads-guilty>> accessed November 2016

Chulov, M. (The Guardian, 15 June 2014) *How an arrest in Iraq revealed Isis's \$2bn jihadist network*, <<https://www.theguardian.com/world/2014/jun/15/iraq-isis-arrest-jihadists-wealth-power>> accessed November 2016

Clark, A. (The Guardian, 30 September 2009) *Betonsports Chief David Carruthers changes guilty plea in the US* <<http://www.guardian.co.uk/world/2009/sep/30/betonsports-boss-changes-guilty-plea-in-us>> accessed November 2016

Delmar-Morgan, A. (The Guardian, 22 July 2015) *Islamic charities in UK fear they are being unfairly targeted over extremism* <[https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share\\_btn\\_link](https://www.theguardian.com/society/2015/jul/22/muslim-charities-uk-targeted-extremism-fears?CMP=share_btn_link)> accessed November 2016

Dodd, V. (The Guardian, 22 September 2015) *School questioned Muslim pupil about Isis after discussion on eco-activism* <<https://www.theguardian.com/education/2015/sep/22/school-questioned-muslim-pupil-about-isis-after-discussion-on-eco-activism>> accessed November 2016

Doward, J. (The Guardian, 9 September 2012) *Peer raises fears over UK charity's alleged links to Boko Haram* <<https://www.theguardian.com/world/2012/sep/09/uk-charity-boko-haram>> accessed November 2016

Elgot, J. (The Guardian, 2 October 2015) *UK schoolboy given life sentence for Australia terror plot* <<https://www.theguardian.com/world/2015/oct/02/uk-schoolboy-life-sentence-australia-terror-plot>> accessed November 2016

Gayle, D. (The Guardian, 21 April 2016) *Prevent strategy 'could end up promoting extremism'* <<https://www.theguardian.com/politics/2016/apr/21/government-prevent-strategy-promoting-extremism-maina-kiai>> accessed November 2016

Glanville, J. (The Guardian, 17 November 2008) *The big business of net censorship* <<https://www.theguardian.com/commentisfree/2008/nov/17/censorship-internet>> accessed November 2016

Greenwald, G & MacAskill, E. (The Guardian, 7 June 2013) *NSA Prism program taps into user data of Apple, Google and others* <<http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>> accessed November 2016

Greenwald, G. & Ball, J. (The Guardian, 21 June 2013) *The top secret rules that allow the NSA to use US data without a warrant* <<http://www.guardian.co.uk/world/2013/jun/20/fisa-court-nsa-without-warrant>> accessed November 2016

Halliday, J. (The Guardian, 20 March 2016) *Almost 4,000 people referred to UK de-radicalisation scheme last year* <<https://www.theguardian.com/uk-news/2016/mar/20/almost-4000-people-were-referred-to-uk-deradicalisation-scheme-channel-last-year>> accessed November 2016

Henley J. and Dodd, V. (The Guardian, 12 August 2016) *Kadiza Sultana: London schoolgirl who joined Isis believed killed in Syria airstrike* <<https://www.theguardian.com/uk-news/2016/aug/11/london-schoolgirl-kadiza-sultana-who-joined-isis-believed-killed-in-syria-airstrike>> accessed November 2016

Hopkins, N. (The Guardian, 8 July 2013) *NSA and GCHQ spy programmes face legal challenge* <<http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge>> accessed November 2016

Hopkins, N. (The Guardian, 24 January 2014) *Justify GCHQ mass surveillance, European court tells ministers* <<http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights>> accessed November 2016

Hopkins, N. & Borger, J. (The Guardian, 1 August 2013) *Exclusive: NSA pays £100m in secret funding to GCHQ* <<http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>> accessed November 2016

Johnson B. & Arthur, C. (The Guardian, 9 December 2008), *British censor reverses Wikipedia ban* <<https://www.theguardian.com/technology/2008/dec/09/wikipedia-ban-reversed>> accessed November 2016



Jones, S. & Siddique, H. (The Guardian, 13 December 2010) *Stockholm suicide bomber confronted by Luton mosque leaders* <<https://www.theguardian.com/world/2010/dec/13/stockholm-suicide-bomber-luton-mosque>> accessed November 2016

Malik, S. (The Guardian, 7 December 2015) *The Isis papers: leaked documents show how Isis is building its state* <<https://www.theguardian.com/world/2015/dec/07/leaked-isis-document-reveals-plan-building-state-syria>> accessed November 2016

MacAskill, E., Borger, J., Hopkins, N., Davies, N. & Ball, J. (The Guardian, 21 June 2013) *GCHQ taps fibre-optic cables for secret access to world's communications* <<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>> accessed November 2016

McCarthy, T. (The Guardian, 18 June 2013) *NSA chief says exposure of surveillance programs has 'irreversible' impact - as it happened* <<http://www.guardian.co.uk/world/2013/jun/18/nsa-chief-house-hearing-surveillance-live>> accessed November 2016

Neate, R. (The Guardian, 11 July 2016) *HSBC escaped US money-laundering charges after Osborne's intervention* <<https://www.theguardian.com/business/2016/jul/11/hsbc-us-money-laundering-george-osborne-report>> accessed November 2016

Owen, P. (The Guardian, 3 June 2010) *George Bush admits US waterboarded 9/11 mastermind* <<http://www.guardian.co.uk/world/2010/jun/03/george-bush-us-waterboarded-terror-mastermind>> accessed November 2016

Pilkington, E. & Watt, N. (The Guardian, 12 June 2013) *NSA surveillance played little role in foiling terror plots, say experts* <<http://www.guardian.co.uk/world/2013/jun/12/nsa-surveillance-data-terror-attack>> accessed November 2016

Qunn, B. (The Guardian, 11 March 2016) *Nursery 'raised fears of radicalisation over boy's cucumber drawing'* <<https://www.theguardian.com/uk-news/2016/mar/11/nursery-radicalisation-fears-boys-cucumber-drawing-cooker-bomb>> accessed November 2016

Ramesh, R. (The Guardian, 16 November 2014) *Quarter of Charity Commission inquiries target Muslim groups* <<https://www.theguardian.com/society/2014/nov/16/charity-commission-inquiries-muslim-groups>> accessed November 2016

Smith, D. (The Guardian, 29 September 2016) *Congress overrides Obama's veto of 9/11 bill letting families sue Saudi Arabia* <<https://www.theguardian.com/us-news/2016/sep/28/senate-obama-veto-september-11-bill-saudi-arabia>> accessed November 2016



Smith, D. & Ackerman, S. (The Guardian, 15 July 2016) *9/11 report's classified '28 pages' about potential Saudi Arabia ties released* <<https://www.theguardian.com/us-news/2016/jul/15/911-report-saudi-arabia-28-pages-released>> accessed November 2016

Travis, A. (The Guardian, 11 May 2007) *Warning on Terrorist Charity* <<http://www.guardian.co.uk/uk/2007/may/11/terrorism.voluntarysector>> accessed November 2016

Treanor, J. (The Guardian, 26 March 2012) *Queen's banker fined for poor money laundering checks* <<https://www.theguardian.com/business/2012/mar/26/coutts-fined-money-laundering-checks>> accessed November 2016

Wainwright, M. (The Guardian, 12 March 2008) *Friend of 7/7 bombers jailed for possessing al-Qaida CD* <<https://www.theguardian.com/uk/2008/mar/12/uksecurity.alqaida>> accessed November 2016

Williams, Z. (The Guardian, 27 June 2014) *The radicalisation of Samantha Lewthwaite, the Aylesbury schoolgirl who became the 'white widow'* <<https://www.theguardian.com/uk-news/2014/jun/27/what-radicalised-samantha-lewthwaite-77-london-bombings>> accessed November 2016

## **The Independent**

Boulton D. (The Independent, 4 January 2016) *Child in Isis video is 'son of female British fanatic' with links to Lee Rigby killers* <<http://www.independent.co.uk/news/uk/home-news/isa-dare-isis-video-grace-khadija-dare-lee-rigby-a6796376.html>> accessed November 2016

Dearden, L. (The Independent, 12 August 2016) *Isis' British brides: What we know about the girls and women still in Syria after the death of Kadiza Sultana* <<http://www.independent.co.uk/news/uk/home-news/isis-british-brides-kadiza-sultana-girls-women-syria-married-death-killed-aqsa-mahmood-islamic-state-a7187751.html>> accessed November 2016

Jeory, T. & Cockburn, H. (The Independent, 23 July 2016) *More than 500,000 public sector workers put through Prevent counter-terror training in bid to spot extremism* ,<http://www.independent.co.uk/news/uk/crime/extremism-prevent-counter-terror-training-public-sector-workers-bid-to-spot-a7152466.html>> accessed November 2016

Mortimer, C. (The Independent, 17 December 2015) *More than 1,000 extremist websites taken down every week London Police Chief Sir Bernard Hogan-Howe says* <<http://www.independent.co.uk/news/uk/crime/more-than-1000-extremist-websites-taken-down-every-week-london-police-chief-sir-bernard-hogan-howe-a6776961.html>> accessed November 2016

Osborne S. (The Independent 5 September 2016) *Australian teen Sevdet Besim jailed for Anzac Day terror plot* <<http://www.independent.co.uk/news/world/australasia/australian-teen-sevdet-ramadan-besim-jailed-anzac-day-terror-plot-melbourne-dandenong-a7226891.html>> accessed November 2016

Sims, A. (The Independent, 25 May 2016) *Sally Jones: Isis recruiter 'issues series of terror threats against UK cities' over Twitter* <<http://www.independent.co.uk/news/world/middle-east/sally-jones-isis-recruiter-issues-series-of-terror-threats-to-uk-cities-over-twitter-a7049066.html>> accessed November 2016

## **The Telegraph**

Professor Paul Wilkinson (The Telegraph, 1 September 1992)

The Telegraph *How terrorists are using social media* (4 November 2014) <<http://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html>> accessed November 2016

The Telegraph (21 October 2016) *Muslim convert who partially blew himself up in a Giraffe restaurant in a failed suicide attack found dead in prison* <<http://www.telegraph.co.uk/news/2016/10/21/muslim-convert-who-tried-to-blow-up-restaurant-with-nail-bomb-fo/>> accessed November 2016

Barratt D. (The Telegraph, 11 March 2016) *Four-year-old who 'mispronounced the word cucumber' threatened with counter-terrorism measures* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12191543/Four-year-old-who-mispronounced-the-word-cucumber-threatened-with-counter-terrorism-measures.html>> accessed November 2016

Beaumont, C. & Martin, N. (The Telegraph, 10 December 2008) *Wikipedia ban lifted by Internet Watch Foundation* <<http://www.telegraph.co.uk/technology/news/3700396/Wikipedia-ban-lifted-by-Internet-Watch-Foundation.html>> accessed November 2016

Boyle, D. (The Telegraph, 9 June 2016) *Parents of 'Jihadi Jack' Letts who was 'first white Briton to join Isis' remanded in custody after denying sending him money for terrorism* <<http://www.telegraph.co.uk/news/2016/06/09/parents-of-jihadi-jack-letts-who-was-first-white-briton-to-join/>> accessed November 2016

Gardham, D. (The Telegraph, 18 July 2009) *Terrorist Andrew Ibrahim was turned in by the Muslim community* <<http://www.telegraph.co.uk/news/5851168/Terrorist-Andrew-Ibrahim-was-turned-in-by-the-Muslim-community.html>> accessed November 2016

Gilligan A. (The Telegraph, 25 December 2010) *Charity Watchdog loses its bite* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8225028/Charity-watchdog-loses-its-bite.html>> accessed November 2016

Goodman, M. (The Telegraph, 29 March 2012) *Coutts agrees to settle FSA fine for reduced fee* <<http://www.telegraph.co.uk/finance/personalfinance/expat->

[money/9173401/Coutts-agrees-to-settle-FSA-fine-for-reduced-fee.html](http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1359800/Anthrax-attack-hits-Congress.html)> accessed November 2016

Harden, T. (The Telegraph, 18 October 2001) *Anthrax attack hits Congress* <<http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1359800/Anthrax-attack-hits-Congress.html>> accessed November 2016

Hope, C. (The Telegraph, 19 March 2009) *Home Office fails to shut down a single extremist website in two years* <<http://www.telegraph.co.uk/news/uknews/de-fence/5017764/Home-Office-fails-to-shut-down-a-single-extremist-website-in-two-years.html>> accessed November 2016

Hough, A. (The Telegraph, 29 February 2012) *Samantha Lewthwaite: 7/7 bomber widow previously a 'Home Counties' girl* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9112824/Samantha-Lewthwaite-77-bomber-widow-previously-a-Home-Counties-girl.html>> accessed November 2016

Palazzo, C. (The Telegraph, 21 July 2016) *Islamic State threatens to intensify attacks against France* <<http://www.telegraph.co.uk/news/2016/07/21/islamic-state-threatens-to-intensify-attacks-against-france/>> accessed November 2016

Pflanz, M. (The Telegraph, 8 July 2012) *Samantha Lewthwaite 'recruiting all-women terror squads'* <<http://www.telegraph.co.uk/news/worldnews/africaandindianocean/somalia/9384893/Samantha-Lewthwaite-recruiting-all-women-terror-squads.html>> accessed November 2016

Raynor, G. (The Telegraph, 4 January 2016) *'Jihadi Junior' confirmed to be Isa Dare, son of female British fanatic with links to Lee Rigby killers* <<http://www.telegraph.co.uk/news/worldnews/islamic-state/12080134/Jihadi-Junior-son-of-female-British-fanatic-with-links-to-Lee-Rigby-killers.html>> accessed November 2016

Ross, T. (The Telegraph, 11 January 2015) *Muslim charity stripped of state funding over extremism fears* <<http://www.telegraph.co.uk/news/politics/conservative/11337846/Muslim-charity-stripped-of-state-funding-over-extremism-fears.html>> accessed November 2016

Shute J. (The Telegraph, 9 January 2016) *How Isil are preying on female converts in Britain to make them into jihadi brides* <<http://www.telegraph.co.uk/news/world-news/islamic-state/12089882/How-Isil-are-preying-on-female-converts-in-Britain-to-make-them-into-jihadi-brides.html>> accessed November 2016

Spencer, R. (The Telegraph, 16 April 2013) *Boston Marathon bombs: al-Qaeda's Inspire magazine taught pressure cooker bomb-making techniques* <<http://www.telegraph.co.uk/news/worldnews/al-qaeda/9998886/Boston-Marathon-bombs-al-Qaedas-Inspire-magazine-taught-pressure-cooker-bomb-making-techniques.html>> accessed November 2016

Spencer, R. (The Telegraph, 3 February 2015) *Target practice: Teenage British twins train in Syria* <<http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11387424/Target-practice-Teenage-British-twins-train-in-Syria.html>> accessed November 2016

Turner, C. (The Telegraph, 23 September 2014) *Government donation to Muslim Charities Forum denounced as "madness"* <<http://www.telegraph.co.uk/news/uknews/11114599/Government-donation-to-Muslim-Charities-Forum-denounced-as-madness.html>> accessed November 2016

Whitehead, T. (The Telegraph, 8 April 2014) *GCHQ given all clear over Edward Snowden allegations by watchdog* <<http://www.telegraph.co.uk/news/uknews/law-and-order/10752205/GCHQ-given-all-clear-over-Edward-Snowden-allegations-by-watchdog.html>> accessed November 2016

Whitehead, T. (The Telegraph, 19 June 2014) *Isis operating like a multinational company* <<http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/10911412/Isis-operating-like-a-multinational-company.html>> accessed November 2016

Whitehead, T. (The Telegraph, 25 January 2016) *Parents of 'Jihadi Jack' speak of two years of hell and daily worry that he could die* <<http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/12120165/Parents-of-Jihadi-Jack-speak-of-two-years-of-hell-and-daily-worry-that-he-could-die.html>> accessed November 2016

## **Time Magazine**

Bager, J. (Time, 6 February 2015) *Saudi Women Right-to-Drive Activists Deploy Twitter, Face Terrorism Court* <<http://time.com/3697073/saudi-arabia-women-drive-twitter/>> accessed November 2016

## **The Times**

Brown, D. (The Times, 29 February 2012) *'I just wanted to marry a Muslim and settle down'* <<http://www.thetimes.co.uk/tto/news/uk/crime/article3335196.ece>> accessed November 2016

## **USA Today**

Eisler, P. (USA Today, 10 July 2008) *Senate OKs Surveillance Revamp* <[www.usatoday.com/printedition/news/20080710/a\\_fisa10.art.htm](http://www.usatoday.com/printedition/news/20080710/a_fisa10.art.htm)> accessed November 2016

## **Wall Street Journal**

Wall Street Journal *Transcript: Obama's remarks on NSA controversy* (Blog, 7 June 2013) <<http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/>> accessed November 2016

Simpson, G.R. (Wall Street Journal, 26 July 2007) *U.S. Tracks Saudi Bank Favored by Extremists* <<http://www.wsj.com/articles/SB118530038250476405>> accessed November 2016

## **Washington Post**

Washington Post (8 October 2001) *Text: Attorney General John Ashcroft* <[http://www.washingtonpost.com/wp-srv/nation/attacked/transcripts/ashcroft\\_100801.htm](http://www.washingtonpost.com/wp-srv/nation/attacked/transcripts/ashcroft_100801.htm)> accessed November 2016

Washington Post *Ashcroft's Pre-9/11 Priorities scrutinised* (12 April 2004) <[http://www.washingtonpost.com/wp-dyn/articles/A6589-2004Apr12\\_2.html](http://www.washingtonpost.com/wp-dyn/articles/A6589-2004Apr12_2.html)> accessed November 2016

Barnes, R. (Washington Post, 7 June 2013) *Secrecy of surveillance programs blunt challenges about legality* <[http://articles.washingtonpost.com/2013-06-07/politics/39815715\\_1\\_warrantless-surveillance-government-surveillance-president-obama](http://articles.washingtonpost.com/2013-06-07/politics/39815715_1_warrantless-surveillance-government-surveillance-president-obama)> accessed November 2016

Finn, P. (Washington Post, 2 May 2012) *Inspire, al-Qaeda's English-language magazine, returns without editor Awlaki* <[https://www.washingtonpost.com/world/national-security/inspire-al-qaedas-english-language-magazine-returns-without-editor-awlaki/2012/05/02/gIQAiEPMxT\\_story.html](https://www.washingtonpost.com/world/national-security/inspire-al-qaedas-english-language-magazine-returns-without-editor-awlaki/2012/05/02/gIQAiEPMxT_story.html)> accessed November 2016

Nakashima, E. (Washington Post, 26 October 2011) *FBI going to court more often to get personal Internet-usage data* <[http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM\\_story.html](http://www.washingtonpost.com/world/national-security/fbi-going-to-court-more-often-to-get-personal-internet-usage-data/2011/10/25/gIQAM7s2GM_story.html)> accessed November 2016

Ross, J. (Washington Post, 19 August 2015) *How Black Lives Matter moved from a hashtag to a real political force* <<https://www.washingtonpost.com/news/the-fix/wp/2015/08/19/how-black-lives-matter-moved-from-a-hashtag-to-a-real-political-force/>> accessed November 2016

Sipress, A. (Washington Post 16 December 2004) *An Indonesian's Prison Memoir Takes Holy War Into Cyberspace* <<http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html>> accessed November 2016

Warrick, J. & Horwitz, S. (Washington Post, 16 April 2013) *Boston Marathon bombs had simple but harmful design, early clues indicate* <[https://www.washingtonpost.com/world/national-security/boston-marathon-bombs-had-simple-but-harmful-design-early-clues-indicate/2013/04/16/c2b061cc-a6d8-11e2-8302-3c7e0ea97057\\_story.html](https://www.washingtonpost.com/world/national-security/boston-marathon-bombs-had-simple-but-harmful-design-early-clues-indicate/2013/04/16/c2b061cc-a6d8-11e2-8302-3c7e0ea97057_story.html)> accessed November 2016

## **Washington Times**

Blake, A. (The Washington Times, 18 November 2016) *Obama shrugs off Edward Snowden's plea for Presidential pardon* <<http://www.washington-times.com/news/2016/nov/18/obama-refuses-edward-snowdens-plea-presidential-pa/>> accessed November 2016

