Home Affairs Committee: Written evidence

Counter-terrorism

This volume contains the written evidence accepted by the Home Affairs Committee for the Counter-terrorism inquiry.

As at 8 April 2014

Written evidence submitted by CST [CT 01]

Letter from Richard Benson, Chief Executive, CST, to the Chair of the Committee, 14 June 2013

In response to your request for information concerning extremist speakers at UK universities for the Home Affairs Committee's inquiry into international terrorism and crime, please find attached CST's submission.

As you will see, we are aware of several incidences of extremist speakers and antisemitic incidents at UK universities that affect the well being of both Jewish students and the wider student community.

Richard Benson, Chief Executive
CST
June 2013

BACKGROUND TRENDS

British campuses are generally places where Jewish students feel safe to study and do not suffer antisemitism on a daily basis. However, there are occasions at some Universities and Students' Unions when Jewish students have been exposed to hate preachers, extremist groups, radicalised individuals, disruption of Jewish Society events and even direct incidents of antisemitism. Extremist activity can leave students from a range of minorities feeling vulnerable and reluctant to express their identity openly. Antisemitism, when it occurs, often takes place in a context that includes other forms of bigotry and as such targets all minority students, and therefore the student body as a whole.

This academic year (2012-13) has seen an increase in far right activity on campus. Some of this increase is part of a cycle of extremism between far right and Islamist extremists

1. PROBLEMATIC SPEAKERS

ISLAMIST SPEAKERS:

- **Haitham Al-Haddad** spoke at Edinburgh Napier University in November 2011 and Roehampton University in May 2012[1]. Al-Haddad was also meant to address students at LSE in February 2012, but his participation in the event was subsequently cancelled.[2] Haitham al-Haddad used facilities at Nottingham campus to host a family retreat weekend in April 2013, the first of a three part course.[3]

  Al-Haddad is the chairman of London's Muslim Research and Development Foundation, a group that gives Sharia advice on financial matters.[4] Al-Haddad has been embroiled in controversy surrounding comments allegedly made in 2001 where it is alleged that he claimed Jews "are the enemies of God and descendants of apes and pigs".[5][6][7] He has persistently denied making those comments. An English-language article by Al-Haddad opposes the actions of Al Qaeda but explains that regardless of what Osama bin Laden did, or did not do, "it is an established part of our Islamic

[1] http://www.youtube.com/watch?v=u5b0V49VusY
[2] http://www2.lse.ac.uk/publicEvents/events/2012/02/20120207t1830vCLM502.aspx
[3] http://www.familyretreat.co.uk/speakers/shaykh-dr-haitham-al-haddad/
[4] http://www.mrdf.co.uk/
[5] http://www.rnw.nl/english/article/cleric-did-say-"jews-are-descendants-apes-and-pigs"
[6] http://www.alminbar.net/alkhutab/khutbaa.asp?mediaURL=4359
[7] http://hurryupharry.org/2012/02/04/more-wisdom-of-haitham-al-haddad/

creed that every Muslim, unlike the disbelievers, will eventually enter paradise". The article also shows various perspectives on what constitutes a "martyr" in combat between Muslims and non-Muslims.[8] Speaking in English, Al-Haddad may be seen on youtube, discussing "why marriages fail". This includes his saying that no outsider should ask a husband why he is beating his wife, because such matters should be sorted between the couple.[9]

- **Azzam Tamimi** has repeatedly appeared on university campuses. Tamimi is spokesperson for the Muslim Association of Britain, director of the Institute of Islamic Political Thought[10]. His Guardian profile states that he has "advised Hamas on media strategy".[11]

  In February 2010, Tamimi was a speaker at the Federation of Student Islamic Society (FOSIS) Palestine Conference[12] held at Manchester University, an Islamic Society event at Cambridge[13] and a Palestinian Society event at SOAS.[14] During his address to SOAS students, Tamimi called for the destruction of Israel and stated,

  "Today Hamas is considered a terrorist organisation because that's what the Americans and Israelis and cowardly politicians of Europe want, but what is so terrorist about it?

  "You shouldn't be afraid of being labelled extreme, radical or terrorist. If fighting for your home land is terrorism, I take pride in being a terrorist. The Koran tells me if I die for my homeland, I'm a martyr and I long to be a martyr."15.

  In November 2004, Tamimi told the BBC's *Hardtalk*:

  "If I can go to Palestine and sacrifice myself I would do it. Why not?...sacrificing myself for Palestine is a noble cause. It is the straight way to pleasing my God and I would do it if I had the opportunity"[16]

- Following the threat of protests by Reading University's Islam Awareness week in February 2013 saw the cancellation of a talk by Uthman Lateef, , due to fear of protests and disruption.[17]

  Uthman Lateef is a preacher from the Hittin Institute.[18] Lateef is alleged to have said, "we don't accept homosexuality...we hate it because Allan hates it".[19] In January and June 2009, Lateef was an advertised speaker at events where Anwar Al-Awlaki (a senior Al-Qaeda figure, later killed by a US drone strike) gave presentations via video link.[20][21]

FAR RIGHT ACTIVITY ON CAMPUS

- **Nick Griffin**, leader of the British National Party, has been invited to university campuses several times in recent years. In February 2012, the Philosophical Society at University College Cork invited Griffin to debate with students; the society withdrew their invitation only days in advance of the

[8] http://www.islam21c.com/politics/2644-advice-to-muslims-on-the-death-of-osama-bin-ladin
[9] See from 9:00 minutes for relevant comments http://www.youtube.com/watch?feature=player_embedded&v=z37H-NuyY1c,
[10] http://www.guardian.co.uk/world/2005/jan/07/iraq.comment
[11] http://www.guardian.co.uk/commentisfree/2008/nov/21/israel-palestine-gaza
[12] https://www.facebook.com/events/280300288948/
[13] http://www.tcs.cam.ac.uk/issue/news/university-islamic-society-accused-of-hypocrisy/
[14] https://www.facebook.com/events/271049642285/
[15] http://www.thejc.com/news/uk-news/27106/calls-destruction-israel-soas-lecture
[16] *Hardtalk*, BBC News 24, 2/11/04, http://news.bbc.co.uk/1/hi/programmes/hardtalk/3985403.stm
[17] http://www.reading.ac.uk/news-and-events/releases/PR490014.aspx
[18] http://www.youtube.com/watch?v=kHEaL6Fs7RA
[19] http://blogs.telegraph.co.uk/news/andrewgilligan/100077810/east-london-mosque-keeps-on-lying/
[20] http://theendoftime.eventbrite.com/
[21] http://www.hurryupharry.org/wp-content/uploads/2010/03/wasatiyyah.jpeg

event[22]. In October 2011, Griffin was invited to address students at Trinity University before again having his invitation rescinded.[23] In October 2012, Griffin was handed a platform at Leeds University after the student newspaper the *Leeds Student* published an interview between themselves and Griffin.[24]

- In February 2013, the Cambridge Union invited **Marine Le Pen** of the French Front National. Around 200 students protested against her presence, but the event proceeded.[25]

- **Jack Buckby**, a student at Liverpool University, founded The National Culturalists society in 2012, renamed as Culturalist Hub in April 2013[26]. Buckby spoke at the 2012 Alliance of European National Movements meeting, explaining how nationalism could be better presented to students, fore xample by its slogan "love culture, hate racism". He was introduced by Nick Griffin, but has declared himself unaffiliated with the BNP[27].

- During a 'Pimps and Hoes' themed bar crawl by Manchester's Varsity Leisure Group, a number of students were spotting donning racist graffiti and messages of support for the BNP on their official bar crawl t-shirts[28].

2. DISRUPTION OF EVENTS

Although the disruption of Israel-related events may not be antisemitic per se, it contributes to an environment of tension, hostility and discomfort for Jewish students; often resulting in Jewish students feeling intimidated and unable to express their views or identities on their own campus.

- In December 2010 at an event at LSE, Abdul Bari Atwan, editor of *Al-Quds Al-Arabi*, responded angrily to questions from Jewish and pro-Israel students, saying "you are bombing us every day". He then spoke of an Iraqi presidential candidate having been "groomed by the Jewish lobby, by the Israel lobby, by the Zionist lobby".[29] He later denied having meant any of this in an antisemitic manner. Atwan refused to withdraw a comment he had made in 2007, that he would "go to Trafalgar Square and dance with delight" if Iranian missiles struck Israel.[30] Atwan's lecture caused such offence that Jewish students walked out of the meeting. This followed the Students' Union Anti-Racism-Anti-Fascism Officer's citing how Atwan's speech had breached the union's own definition of antisemitism.[31]

- In April 2013, a venue booked to host the St. Andrews University Jewish Society's Ball received numerous abusive and threatening phone calls, objecting to the recipients of funds to be raised by the event, including Friends of the Israeli Defence Forces.

- In February 2013, George Galloway MP addressed students in Oxford giving his opening speech of an agreed debate about Israel. Galloway walked out of the debate without even engaging with his opponent, Eylon Aslan-Levy, after discovering Aslan-Levy is an Israeli national.[32]

[22] http://corkindependent.com/stories/item/7110/2012-4/Nick-Griffin-UCC-visit-%E2%80%98threat-to-safety%E2%80%99
[23] http://www.guardian.co.uk/commentisfree/2011/oct/17/nick-griffin-trinity-college-dublin
[24] http://www.leedsstudent.org/2012-10-26/ls1/leeds-student-speaks-to-nick-griffin-leader-of-the-bnp
[25] http://www.telegraph.co.uk/education/universityeducation/student-life/9881110/Marine-Le-Pen-sparks-Cambridge-protests.html
[26] https://twitter.com/culturisthub
[27] http://www.youtube.com/watch?v=gooUZ2iD_Pw
[28] http://www.manchestereveningnews.co.uk/news/greater-manchester-news/students-on-pimps-and-hoes-bar-crawl-800859
[29] See 00:12:29 http://www.youtube.com/watch?v=xOJ8LT7DlfA,
[30] http://www.jpost.com/International/Article.aspx?id=73549,
[31] http://thebeaveronline.co.uk/2010/12/07/abdel-bari-atwan-talk-sees-students-walk-out/
[32] http://www.guardian.co.uk/politics/2013/feb/21/george-galloway-debate-israeli-oxford

- In February 2013, Israeli deputy Ambassador Alon Roth-Snir was greeted by about 70 protestors outside his lecture at Essex University. Approximately 40 people disrupted the meeting itself, forcing security officers to evacuate the speaker.[33]

- In October 2012 Israeli Ambassador Daniel Taub addressed students at Edinburgh campus. The lecture was abandoned after severe disruptions by approximately 150 protestors.[34]

- In February 2010, Israeli deputy Ambassador Talya Lador-Fresher was due to address students at the University of Manchester, however, due to safety concerns after 300 students arrived to protest her presence, the event was cancelled. Lador-Fresher returned to Manchester to address politics students in April 2010. Approximately 40 students physically attacked her car whilst she was inside.[35]

3. ANTISEMITIC INCIDENTS

Throughout 2012, there were a total of 32 campus-related antisemitic incidents reported to the CST.[36] Of these, 18 took place on campus and 14 affected students or academics off campus. Below are some examples:

- In November 2012, during an anti-Israel demonstration at Birmingham University, a visibly Jewish student was the victim of antisemitic verbal abuse.

- In November 2012, at a Halloween party at Goldsmiths, a student was photographed wearing a Nazi uniform and saluting "Heil Hitler".

- In October 2012, a group of 7 students were harassing a Jewish male student in the corridor of a college in Cambridge. As a Jewish girl walked past to enter her room, one of the seven turned to her, directly addressed her as 'a Jew' and slapped her across the face.

- In March 2012, a UCL Jewish student was campaigning for a seat on the Students' Union. Swastikas were drawn over some of his posters. In February 2012, it was reported that a swastika was graffitied onto a lift in the UCL library.

- In January 2012, the LSE rugby club played a Nazi drinking game during an organised winter skiing holiday. A Jewish student in the group was subjected to antisemitic abuse and later had his nose broken.[37]

4. GROUPS KNOWN TO HAVE HARBOURED EXTREMISM:

Hizb ut-Tahrir

Hizb ut-Tahrir is an Islamist organisation that has a record of offensive and inflammatory statements regarding Jews, non-Muslims, and gay people, amongst others. They were added to the NUS No Platform policy in 2004, which denies them the ability to be involved with the national union. However, this policy only has an advisory capacity for individual Students' Unions. Since then, the organisation has regained some of its presence on campus via front-groups:

[33] http://www.thejc.com/news/uk-news/102638/israels-deputy-ambassador-forced-flee-essex-university-lecture
[34] http://www.thejc.com/news/uk-news/88068/university-students-disrupt-israeli-ambassador-talk
[35] http://www.thejc.com/news/uk-news/31165/israel-deputy-ambassador-shocked-manchester-attack
[36] http://www.thecst.org.uk/docs/Incidents%20Report%202012.pdf (p.19)
http://www.thecst.org.uk/docs/CST%20Incidents%20Report_Jan-June%202012.pdf, p.5.
[37] http://www.thejc.com/news/uk-news/62277/nazi-students-hit-protester-lse-ski-trip

- Suspected Hizb ut-Tahrir front groups have names such as Perspective Societies, Ideology Societies and Belief and Reason.[38] Such groups have been identified in Manchester and various London universities including SOAS[39], Westminster[40], Imperial[41], City[42] and Queen Mary[43].

- In April 2011, two suspected Hizb ut-Tahrir activists were voted onto the Westminster Student Union as President and Vice-President of Education, respectively. They have been banned from attending NUS events.[44]

- In February 2013, Shohana Khan, the Women's Deputy Media Representative for Hizb ut-Tahrir, spoke at an event at City University[45].

Muslim Public Affairs Committee:

The Muslim Public Affairs Committee (MPAC) website includes anti-Zionist conspiracy theorising. In 2006, Asghar Bukhari, a founder of MPAC and its spokesman, was shown to have given money to Holocaust revisionist, David Irving in 2000; and urged others to do likewise. Bukhari stated this was because he had regarded Irving as "anti-Zionist". In 2004, the National Union of Students described MPAC as antisemitic and banned the group.[46]

- Asghar Bukhari spoke at an event on 6th February 2013 at Middlesex University alongside John Rees of the Stop the War Coalition and the journalist Lauren Booth.
    - Due to surrounding controversy over the speakers, the event was restricted to registered Middlesex students only.

Following the presence of MPAC at Middlesex University, the Students' Union held a referendum to reaffirm the Union's policy of not providing a platform for individuals with racist or fascist views (26th-27th February 2013) which received 73% voting yes.[47]

CST

June 2013

[38] http://www.huffingtonpost.co.uk/alexander-meleagrouhitchens/the-future-of-campus-extr_b_1082401.html
[39] http://www.youtube.com/watch?v=3yKd8ZAymGU
[40] https://www.facebook.com/global.ideas.soc?ref=ts&fref=ts
[41] https://www.facebook.com/#!/groups/143279022374652/
[42] http://www.youtube.com/watch?v=VUHFAXnVbWE
[43] https://www.facebook.com/#!/groups/QM.Ideological.Society/
[44] http://www.thejc.com/news/uk-news/47884/students-elect-two-who-back-caliphate,
[45] http://www.youtube.com/watch?v=LxCNMRgqXNQ
[46] http://www.guardian.co.uk/uk/2006/nov/19/secondworldwar.religion
[47] http://www.musu.mdx.ac.uk/uploads//No%20Platform%20Policy.pdf

Written evidence submitted by
Cressida Dick, Assistant Commissioner, Metropolitan Police [CT 02]

Update by Assistant Commissioner Cressida Dick on the murder of Drummer Lee Rigby

Follow up action

I believe there were two undertakings for follow-up action from Assistant Commissioner Cressida Dick. These were in relation to the Counter-Terrorist Internet Referral Unit (CTIRU) and the Certificate in Knowledge of Policing (CKP). I attach a brief note on both, which I hope will address the Committee's interest. Please let me know if you require anything further.

The Counter Terrorism Internet Referral Unit (CTIRU)

The Counter Terrorism Internet Referral Unit (CTIRU) is part of the Counter Terrorism Command and holds the national remit for assessing terrorist and violent extremist material on the internet. The unit is proactive in its approach to terrorist content but also receives referrals through a public online reporting tool that allows members of the public to report their concerns anonymously.

It is also be responsible for alerting forces, Counter Terrorism Units and Counter Terrorism Intelligence Units to online terrorist offences that may fall within their jurisdiction. Its aim is to make the internet a more hostile environment for terrorists and violent extremists by making operating conditions more difficult for them. As the vast majority of terrorist content is hosted overseas this includes working with industry and foreign law enforcement agencies to prevent the internet being misused to promote violence.

Since the unit was formed in February 2010 over 5,700 individual pieces of online terrorist content have been removed from the internet and almost 1,000 other links have been filtered from the UK public estate which prevents them from being accessed on computers in locations such as libraries, universities and other publicly funded institutions.

Certificate in Knowledge of Policing

The eligibility requirements to become a new police constable in the police service have changed. As of April 2013 candidates applying to the MPS are required to have completed a Certificate in Knowledge of Policing (CKP) before starting as a constable. The CKP is a self-funded qualification developed by the College of Policing, in partnership with Skills for Justice and all Home Office funded Police Forces, and is broadly equivalent to an A-Level. It covers the wide range of policing and legislative knowledge that constables need to perform their role effectively. It will provide an ideal foundation for a career in policing, ensuring that new police constables have the

knowledge, and understanding as well as the dedication to keep Londoners safe, prior to their in service training.

A CKP will cost approximately between £800-£1,000 to fund and 6 weeks (full-time) to complete. The course is also accessible at weekends and evenings. Further and Higher Education providers as well as independent providers will obtain a licence from the College of Policing to deliver the CKP course. The MPS is currently looking at various financial support packages for candidates, including for example, Bursaries.

The MPS has agreed a range of positive action options as permitted under the Equality Act to help support candidate's individual needs when applying to join as a police constable, enabling us to attract and recruit a more representative workforce of the communities we serve. These include access to coaching by established officers, additional training prior to candidates attending assessment centres and changes to the recruitment processes whereby external BME candidates will be able to take their Day 1 assessment prior to obtaining CKP.

When a candidate's application passes initial checks, they will be invited to attend a formal, day-long assessment referred to as 'Day 1'. The day comprises of:

A competency-based structured interview
A numerical ability test
A verbal ability test
Two written exercises
Four interactive exercises

These activities allow the MPS to observe and assess whether the candidate has the right skills and qualities required to be a police constable.

We know from the 2011 census that London is more diverse than ever and that our workforce does not reflect that diversity as we would like it to. We believe that to police a diverse city like London successfully and with the consent, support and engagement of the communities we serve, we need a workforce that more closely reflects London at all levels.

Improvements have been made to the diversity of our workforce with nearly 10.4% (3,170) of our police officers now from a BME background. However, in order to increase that number, we need to adapt our approach so we see a change in the makeup of our workforce now, not in the distant future. To achieve this we want to use options permitted under the Equalities Act to help target and attract candidates from BME backgrounds into a successful career in the MPS.

The MPS has rigorous selection standards to ensure we recruit officers who are the best fit for the demands of policing our capital now and in the future. These high standards the MPS prides itself on will remain, with the additional requirement of the CKP, as we move into our latest recruitment drive. We will work closely with both

course providers and the College to monitor both uptake and access to funding streams. If certain communities are adversely affected, this intelligence will help shape future recruitment campaigns.

Cressida Dick, Assistant Commissioner, Metropolitan Police
June 2013

Written evidence submitted by
Cressida Dick, Assistant Commissioner, Metropolitan Police [CT 02a]

RE: HASC Inquiry into the PURSUE Strand of CONTEST - CT Policing Contribution

1. I welcome the opportunity to provide written evidence to your inquiry into PURSUE. Policing makes a very considerable contribution to this pillar of the CONTEST agenda and I believe CT Policing capabilities, structures and processes have improved significantly in recent years and continue to evolve.

2. I fully agree with the Home Secretary's recent assertions that whilst the threat of terrorism remains real and sustained, our ability to counter it remains strong. There are several reasons for this, not least that our collective understanding of the threat has broadened and deepened over recent years, improving our ability to detect and disrupt it. In addition to this the increasingly integrated nature of the UK counter terrorism effort, whilst to the outside eye can often look quite complex, is critical in mitigating daily the risk from terrorism.

3. This note sets out briefly how we support activity that seeks to identify, investigate and disrupt terrorist attacks in this country and our interests overseas. I will then turn to the role of our partners and how we integrate operationally and strategically with them, before finally highlighting some current issues which are at the forefront of our thinking. Whilst this is not an exhaustive account of our arrangements, you will notice that it does highlight two critical components, notably structures and collaboration.

THE COUNTER TERRORIST NETWORK

Local

4. There can be a misconception that the Pursue effort begins with counter terrorism specialists. However, the ability to prevent and detect terrorist offences is led within communities and by front line policing. A core part of the neighbourhood officer's role is the ability to build relationships, confidence and trust, which in turn can encourage greater public vigilance, responsiveness and passing of intelligence. It is also front line policing that will be the first to respond to a terrorist attack in a manner which preserves life, safety and evidence and sets the tone for the investigation and wider community confidence.

5. With this in mind we have been committed to developing the relationship with policing at a local level. Doing so has ensured full engagement with the wider police service and local partners - from intelligence assessment to overt responses on the street, from community engagement to the in-force provision of Special Branch Officers. It is worth noting that a significant proportion of Pursue related intelligence leads come from the police, therefore it is vital that we keep casting the net for intelligence gathering as widely as possible, harnessing all our policing capability and strengthening community links.

Regional

6. The local, core policing function is the bedrock upon which we have built specialist CT Policing capability. Force Special Branches units provide the link between local policing activity and the regional hubs that sit above them. These 'parent' hubs divide into two types. Counter Terrorism Intelligence Units (CTIUs) which co-ordinate regional police intelligence resources, whilst Counter Terrorist Units (CTUs) have expanded capabilities to manage major counter terrorism operations and disruption activity.

7. These hubs are located in those geographical areas of highest projected demand, anchored in local forces, which in turn reach back into the communities they serve. At the same time, the CT Network operates collectively as a single national entity and engages with a range of partners, including the Security Service and the Secret Intelligence Service. In particular the relationship with the Security Service, which I reflect on later, has been instrumental in enhancing joint regional working and developing our collective understanding of the threat at a local level.

8. Activity at this level can range from simple disruption activity, such as the seizure of vehicles and prosecution for road tax offences, to full blown covert operations utilising the panoply of covert intelligence-gathering techniques. It is also worth noting at this point, the significant amount of resources and effort required to investigate a terrorist incident. By way of example, I mentioned to you in my appearance before you on 4th June 2013, following the horrific murder of Lee Rigby, that around 600 officers were employed directly on that investigation. More than 150 of these were from the national police CT Network beyond London.

9. A key point here, and often unrecognised, is the sheer number of successful terrorist prosecutions that we have undertaken. Since the tragic events of 11 September 2001, the UK CT effort has been responsible for 330 convictions related to terrorism. The level of skill, knowledge and determination in bringing those people to justice is manifested in the majority of guilty pleas entered (a previously unheard of phenomenon in the history of terrorist-related prosecutions).

National

10. In addition to the capability within CTUs/CTIUs, the police CT Network has a number of units with national responsibilities performing highly specialised roles. They support the wider Prevent and Pursue effort through bespoke, and often cutting edge, capability. An example of this is the Counter Terrorism Internet Referral Unit (CTIRU) whose remit is to ensure the internet is an environment where terrorist and violent extremist messages are challenged. Through its public facing web page and industry links, it seeks to identify and take down extremist online content from a host of platforms ranging from social media to static web sites. Allocating resources to tackle the almost exponential growth of online activity, recognises that radicalisation takes many forms and we must be alive to all of them. Moreover, the figure of over 18,000 takedowns of online content since June 2012 alludes to the scale and complexity of the challenge.

11. In recognition that financing is fundamental in enabling terrorists and extremists to operate at home and overseas, the National Terrorist Financial Investigation Unit (NTFIU) fulfils a key role in providing quick time intelligence and evidence. Understanding how terrorists raise, move, store and use money is an integral part of not only increasing terrorists' vulnerability but also of enhancing our ability to disrupt their activity. More widely the NTFIU has a broader strategic role in contributing to the HMG counter terrorist finance strategy.

12. Whilst much of our effort is focused toward the threat of terrorism from Al Qaeda and its associates, we remain cognisant of the threat from individuals who engage in terrorist activity in the name of Extreme Right or Left wing views or other ideologies. The National Domestic Extremism and Disorder Intelligence Unit (NDEDIU) sets the national strategic direction for understanding extremist threats to the UK. It has a wide range of international partners which it works with, particularly law enforcement and security agencies in Europe. Furthermore it enables us to understand and respond more effectively to the nexus of terrorism and hate crime. For this reason Domestic Extremism policing remains an integral part of CT and wider law enforcement activity.

13. Despite some obvious differences in law, funding and structures, the Network I have described is fully integrated with colleagues in Police Service Scotland and the Police Service of Northern Ireland. We operate to the same standards and processes and have integrated systems and technology wherever possible. The Chief Constables are members of ACPO(TAM) Board and dialogue involving their services is constant. This join-up is a vital part of managing the terrorist threat across the UK.

International

14. To reiterate the recently-expressed view of the Director General of the Security Service, the current terrorist threat is both diverse and diffuse. Moreover, those who seek to do us harm pay little attention to international borders. In recognition of this fact, the police CT Network plays a full and critical role in supporting countries overseas to investigate and prosecute terrorists who may threaten the UK and our interests. Our network of Counter Terrorism and Extremism Liaison Officers (CTELOs) are strategically located and work closely with police counterparts in their host countries and regions.

15. CTELO activity is wide ranging and includes:

- providing assistance in efficiently progressing CT-related enquiries emanating from, and directed into, the UK (this includes working within Europol);
- acting as the forward deployment for UK CT police in respect of terrorist incidents where UK nationals or interests are involved to assist the host country in conducting their investigation;
- mentoring and building effective and human-rights-compliant CT capability within foreign police agencies in support of the FCO Justice and Human Rights Partnership (JHRP) Programme.

16. The CTELO network has already had a significant impact in effectively changing the approach of some JHRP countries towards the way they conduct CT investigations by shifting their focus towards building a sound evidential prosecution case which meets international human rights standards. There is still much more that the UK CT Network can contribute to the Government's overseas strategy in this area and the CT police overseas network will be consolidated and extended further in the months to come. We are

committed to providing assistance and support wherever a CT police officer can work legitimately with our partners to make a significant difference in delivering effective investigative capability.

17. In addition to our overseas footprint we are able to rapidly deploy officers from the CT Network in response to attacks overseas on UK citizens or where there is a UK interest. For example the Counter Terrorist Command in the MPS led the UK response following the terrorist attack on a gas plant processing facility in In Amenas, Algeria in January. You will be aware that six British citizens and one British resident were killed and many more affected. This is an ongoing operation, with extensive support being provided by us to the Foreign Office and the HM Coroner and there continues to be significant family liaison work and engagement with a range of international partners.

18. The deployed team were able to manage the recovery, identification and repatriation of any UK deceased, conduct interviews and evidence gathering from survivors.

19. Led by the Forensic Management Team, the UK set a strategy for the international identification and repatriation of deceased and their remains, managing all aspects of the mortuary process. With the assistance of international partners from Norway and Japan, the team examined a high number of bodies and body parts, conducting all DNA work here in the UK. This process enabled the repatriation of UK and other international victims and all associated body parts to UK Coronial standards. The mortuary process allowed the UK team to support local authorities through the Disaster Victim Identification (DVI) process with the sharing of best practice and the training of local staff. In addition, officers were able to visit the scene and gain an insight into the events of this attack in order to support the coroner.

20. Following the attack on the Westgate shopping centre, the CTELO had been heavily engaged with the Kenyan police response. The decision was taken to deploy a Counter Terrorism Command team of investigators in order to assist the Kenyan police investigation and mentor local resources in the effective examination of a terrorism scene, along with all the issues associated with body recovery to an internationally approved standard.

21. The CTELO has an extremely good relationship with the Anti-Terrorist Police Unit and this allowed the investigation team access to relevant material and allowed for the team to assist local staff with scene examination and body recovery. Previous training has been delivered to the Kenyan police by the Counter Terrorism Command but this was their first major scene. Working alongside the Kenyan police, with the assistance of FBI colleagues, the team were able to mentor them through all aspects of scene management, scene investigation and body recovery. This included mortuary management in mass fatality terrorist attacks.

Governance and Co-ordination

22. Having attempted to give a coherent account of CT structures it may be helpful to describe the overarching governance and coordination arrangements which focus those broad functions toward the strategic aims of Pursue.

23. In the UK, operational command of policing is vested in Chief Constables, however in order to deliver a nationally consistent and collegiate approach, those chief officers have agreed that CT Policing will be overseen by ACPO (Terrorism and Allied Matters) (ACPO TAM). Strategic direction of ACPO(TAM) is set by the ACPO(TAM) Board, chaired my me with Vice Chairs who are Chief Constables from the police forces which host the regional CTUs.

24. Taking a step down from strategic oversight, operational activity is led by the Senior National Coordinator (SNC) who is a Deputy Assistant Commissioner in the Metropolitan Police Service (MPS). The SNC is mandated by all Chief Constables to coordinate major CT investigations nationally. It is the empowerment of the SNC by Chief Constables that ensures that the Network can flex and surge its assets across regions and disrupt threats effectively. It is also a recognition that CT Policing is delivered by consensus and buy-in with all forces being equitable partners.

25. At an operational and tactical level, the ACPO Counter Terrorism Coordination Centre (ACTCC) provides the tasking and coordination function for the national Network. The key role of the ACTCC is to direct assets and operations toward the most critical threats and intelligence in line with the SNC's mandated responsibility. A secondary function is the oversight and scrutiny of this activity through the collation and analysis of national operational demand information, which assists the strategic modelling of resources and ensures that activity is directed to the most appropriate operations and regions.

COLLABORATION AND RELATIONSHIPS

The Security Service

26. The increasingly collaborative and integrated nature of how we operate is a critical component of our ability both to understand and to disrupt terrorist threats. Although the Security Service has the lead role in National Security, it is widely recognised that the close partnership between the police and the Security Service is essential for the effective delivery of PURSUE. It is our ability to work seamlessly and collaboratively together, despite sometimes differing objectives, that makes our unique relationship the envy of the world.

27. The principle of joint working is particularly important in order to reach a shared understanding and prioritisation of the threat. On that basis we have processes in place that allow us to work together to gather intelligence and evidence, continually re-assess the threat and to identify and task potential disruption opportunities. A balance must always be struck between immediate risk mitigation and longer term disruptive impact. Because of our executive powers and experience in mitigating criminal threat, the police play a significant role in disruptions of terrorist networks.

Broader Policing Partners

28. As I have mentioned earlier, the ability of counter terrorist specialist policing to respond effectively to the threat from terrorism relies heavily on the activities of every police officer, community support officer, and member of police staff. Individual instances of police activity can contribute to community confidence that will, in turn, encourage reporting of valuable intelligence and reduce the risks of radicalisation. All front-line staff must respond appropriately to suspicious incidents. They can receive information from the public or partners, and can pass it to CT specialists. This intelligence can be assessed against other local information and against other sensitive intelligence.

29. When police intervene against terrorist suspects, this can inevitably impact on communities. The close integration between officers dealing directly with the suspect, those helping to deal with the family, with neighbours and with the wider community is critical to ensuring this is conducted safely and sensitively whilst respecting operational sensitivities and the rights of the suspect.

30. A powerful example of where an integrated policing response is so effective was following the murder of Mohamed Saleem in April and the planting of bombs outside mosques in Walsall, Wolverhampton and Tipton in June and July. Not only did an excellent terrorism investigation lead to the arrest and charge of Pavlo Lapshyn, a Ukrainian student who subsequently pleaded guilty. But front line policing were instrumental in engaging and reassuring the local Muslim community by visiting over 200 Islamic institutions in the West Midlands to dispense safety advice and reassurance. And when it came to tracking down the offender, specialist counterterrorism officers worked effectively with local police to find and identify him.

31. CT Policing also relies on specialist police activity that is not CT-specific such as firearms policing, forensics, and surveillance. This support can vary in volume significantly. During ‘routine’ investigations, CT assets are allocated in a clear tasking process against an agreed set of priorities. During and after a terrorist incident and at other critical times, the demand for these specialist resources can greatly exceed usual capacity. In those circumstances, support would be drawn from broader policing. It is imperative that in those circumstances, all the assets can operate effectively together and considerable work has been carried out to ensure this works well.

Local Delivery Partners

32. One area which presents options to disrupt the spread of extremist ideology is the police contribution to the Prevent strategy, which is inextricably linked to Pursue. The police contribution includes the implementation of the ‘Channel’ project. Channel is a multi-agency project funded by the Home Office, Office of Security and Counter Terrorism (OSCT). It is aimed at protecting people at risk of radicalisation, through the provision of a mechanism for early intervention to divert them away from being drawn into the commission of terrorist activity. It is only at a local level that we can integrate effectively with those organisations and groups that have a deeper and more credible reach into groups or individuals susceptible to radicalisation. We continue to work hard to build trust and confidence within communities and local partnerships to identify and divert those involved in or vulnerable to radicalisation. We can only deliver effective Channel interventions in close partnership with local partners.

The Crown Prosecution Service

33. The involvement of dedicated specialist prosecutors working closely with police officers from the Counter Terrorism Command and the Counter Terrorism Units around the country is key to one of the fundamental aims of PURSUE, to prosecute terrorists successfully and bring them to justice. Prosecutors from the Special Crime and Counter Terrorism Division of the CPS work with the police and the intelligence agencies from an early stage and in many cases prosecutors advise long before suspects are arrested. This close working practice has helped to build a strong trilateral relationship between prosecutors, police and the intelligence agencies based on mutual respect and trust.

34. It is usual for the prosecutor to be apprised of the intelligence picture from the outset in order to ensure that there is nothing that will adversely affect a prosecution and for prosecutors to advise on how intelligence can be converted to reliable admissible evidence. Advising early on evidence collection and the strength of the on-going investigation, assists law enforcement to take actions to maximise the potential for admissible evidence in any future trial. Prosecutors are also better able to anticipate those areas that might cause them difficulty if they are aware of the whole picture including any sensitive or national security issues from the outset. The importance of these relationships and early engagement must not be underestimated; as I have suggested already, the number of successful investigations and prosecutions that the agencies have achieved together over the last 10 years or so are testament to that.

National Offender Management Service (NOMS)

35. Another key delivery partner is the National Offender Management Service (NOMS). NOMS and CT Policing work in partnership to identify and assess radicalisation and extremism in prisons and jointly to deliver interventions and management of extremist offenders once released back into the community. Key risks that NOMS seeks to help manage include, *inter alia*, a terrorist incident outside prison arranged or conducted from within prison; a terrorist incident taking place inside a prison; a participant in a terrorist incident outside prison found to have been radicalized and or recruited inside prison and; a terrorist/extremist under probation supervision taking part in a terrorist incident.

BORDERS

Importance of Border Controls

36. Law enforcement at our ports and borders plays a core role in protecting the UK and our interests overseas from any act that may jeopardise our security and stability. Intelligence assessments have continually highlighted the significance of international travel and the vulnerability it creates in relation to national security. The predominant threats to the UK now and for the foreseeable future are from International and Northern Ireland Related Terrorism. The ideology, capability and objectives of the main terrorist groups present a complex challenge as to how our borders need to be policed.

Schedule 7

37. Police officers at ports have powers under Schedule 7 of the Terrorism Act 2000 to stop, question, search, and if necessary, detain people entering or leaving the UK. The legislation is used by officers to determine whether a person appears to be (or has been) concerned in the commission, preparation and instigation of acts of terrorism. This power remains a vital tool in our armoury and recent events only serve to highlight the scale and complexity of the threats that pass through ports across the world where there is only a fleeting opportunity to assess whether a person should be stopped and examined further. In simple terms, the use of Schedule 7 has identified many previously unknown persons who have been discovered to be involved in terrorism, and who could have carried out or assisted an attack causing much loss of life and injury*, here or abroad*.

38. Notwithstanding that, we acknowledge that use of this power is a contentious issue for some, and we recognise that appropriate safeguards need to be in place to ensure it the power is exercised proportionately. We have therefore fully engaged in the recent consultation to review the Schedule 7 power and continue to work to add clarity to how it will be used in the future. This includes working to support the development of the new codes of practice. We continue to engage with communities to clarify and explain how and why we use Schedule 7, respond to recommendations from the Independent Reviewer of Terrorism Legislation and where necessary streamline access to the complaints process.

FUTURE CHALLENGES

Managing Residual Threat

39. The police and Security Service have long recognised that, given the finite nature of investigative resources and the intensive resource requirements of counter terrorism investigations, careful prioritisation has to take place to ensure resources are appropriately directed to the areas of greatest risk. However, it has also been recognised that, outside the specific investigations, a mechanism is necessary to analyse and manage the risk posed by individuals who are not subjects of interest within active investigations.

40. The 'Emerging & Residual Threats' (ERT) process is a national programme, being developed jointly by the police and Security Service, to ensure identification and mitigation of the extremist threat at both a regional and national level. The process is based on an integrated police and Security Service assessment process, which considers a more holistic view of risk. This approach is aimed at gaining an understanding of the broad range of issues that affect each particular region.

Communications Data

41. We continue to give a perspective to Government on legislative powers. Communications Data is vital for law enforcement. It is an essential tool in our ability to protect the public and keep people safe from harm. It provides investigative breakthroughs in the most heinous of crimes, including child abuse (in particular large paedophile rings), murder, kidnapping, cyber crime and terrorism offences. Communications data provides evidence that can be put before a court to ensure the successful prosecution of offenders. The necessity to obtain web logs, foreign Internet based data and to resolve IP addresses has not changed; while the usage of web based services increases exponentially.

42. Technology is increasingly moving society towards virtual lifestyles, with 94% of UK adults having access to mobile phones. The duty of law enforcement to protect and investigate when required to do so, is being hindered without the necessary provisions being available. The continuing erosion of this capability, without the necessary legislative changes, will severely impact on our ability to conduct terrorist investigations, with potentially grave consequences.

CONCLUSION

43. There have been numerous and significant counter terrorist disruption operations undertaken in the last few years, many of which have resulted in successful trials. But these also serve to remind us of the scale of the threat posed from those determined to mount attacks against us. Recent events both here and overseas remind us that we can never be complacent. Our national CT Network is continually tested. We played a major role in keeping the 2012 Olympic and Paralympic Games secure. Our preparedness for this left many important legacies, not least improved structures and processes and strengthened relationships with key partners.

44. Underpinning all of our activity and providing the "golden thread" through our national and international reach, is the local, specialist knowledge and ongoing neighbourhood policing efforts, every day, across the country, building confidence and links with communities. Keeping our citizens safe requires us to be effective at our evidence gathering and we can only do this with community confidence and engagement.

45. For obvious reasons, the London Counter Terrorism Command is a very large unit and the Metropolitan Police provides day-to-day strategic leadership and co-ordination through the role of the Assistant Commissioner and Senior National Co-ordinator. But there is no single lead force that delivers CT Policing. It is a truly collaborative endeavour, mandated by all Chief Constables, and one which provides national strategic direction and oversight, through a board of Chief Constables chaired by me, whilst maintaining and harnessing critical links into local policing, in turn anchored to local communities. Our structures allow the broader intelligence community, in particular the Security Service to harness local intelligence and link downstream and upstream intelligence. We are rooted firmly into a myriad of local partners, local authorities and voluntary and statutory agencies. These links are more important than ever in light of the diverse and more localised nature of the threat, the increasing risk posed by self starting individuals and other violent extremists.

46. In late 2012 we initiated a programme of work to consider and provide evidence of what works most effectively across the CT Policing Network and to identify areas of performance requiring further improvement and enhancement. We will continue to improve on what we've built so that we are in the best possible shape to meet the enduring threat we face.

Cressida Dick
Assistant Commissioner
Chair of ACPO TAM

Written evidence submitted by the Foreign and Commonwealth Office [CT 03]

Letter from Rt Hon William Hague MP, Foreign Secretary, to the Chair of the Committee, 16 June 2013

Thank you for your letter of 31 May to Dr Christian Turner, my High Commissioner in Nairobi, about the arrest in November 2010 of Mr Adebolajo, one of the suspects in the murder of Drummer Lee Rigby, as part of the Home Affairs Select Committee's inquiry into countering international terrorism and crime. I understand you have also written regarding the incident to other parts of the Government.

There has been considerable and understandable Parliamentary and media attention on this attack. For that reason the Prime Minister made a statement to the House on 3 June 2013, confirming that a thorough investigation would be conducted by the Intelligence and Security Committee of Parliament (ISC). The ISC is able to receive and consider a wide range of sensitive material from Government departments and agencies, and we have recently expanded its remit and strengthened its role through the Justice and Security Act 2013. The Committee's investigation will cover all aspects of this attack, including the issues you have raised. The ISC hopes to conclude its work on this investigation around the end of the year.

Both I and the Home Secretary believe the ISC is the appropriate forum to consider these matters, and we are confident that its investigation will be comprehensive and robust. I hope you will appreciate that we are keen to avoid opening up a dual track approach to Parliamentary scrutiny. We also want to avoid any prejudice towards the current prosecution of Mr Adebolajo and his co-defendant, and the investigation into other suspects which could result in a criminal prosecution. On this basis we have respectfully decided to decline your request for this information.

I am copying this letter to the Home Secretary and Sir Malcolm Rifkind.

Rt Hon William Hague MP
Foreign Secretary
June 2013

Written evidence submitted by the Home Office [CT 04]

Letter from Rt Hon Theresa May MP, Home Secretary, to the Chair of the Committee, 17 June 2013

HOME OFFICE FUNDING FOR RADICALISATION PREVENTION PROJECTS

Thank you for your letter of 24 May following the attack in Woolwich asking about radicalisation prevention projects in London that work specifically with black converts to Islam.

Under the revised Prevent strategy, local authorities are responsible for identifying project which they consider relevant to the risks in their local areas. We have funded a number of projects put forward by local authorities in London which work with young Muslims, including those who are converts. We do not currently fund any projects which work specifically with black converts, and we have not received any proposals for such funding.

Our approach to protecting vulnerable people builds on Channel, the existing multi-agency programme to identify and provide support to people at risk of radicalisation. Channel is available to all vulnerable people regardless of their ethnic or religious background.

You also asked whether either suspect was known to prevention projects prior to the attack in Woolwich. As there is a criminal investigation underway, I am sure that you will appreciate I am not able to comment further on this at this time.

Rt Hon Theresa May MP
Home Secretary
June 2013

Written evidence submitted by the Home Office [CT 04a]

Letter from Rt Hon Theresa May MP, Home Secretary, to the Chair of the Committee, 24 June 2013

Thank you for your letter to the Security Service, dated 29 May, seeking further information regarding the tragic events in Woolwich on 22 May as part of the Home Affairs Select Committee's inquiry into countering international terrorism and crime.

There has been considerable and understandable Parliamentary and media attention around this attack. For that reason the Prime Minister made a statement to the House on 3 June 2013 confirming that a thorough investigation would be conducted by the Intelligence and Security Committee of Parliament (ISC), chaired by Sir Malcolm Rifkind MP. The ISC is able to receive and consider a wide range of sensitive material from Government departments and agencies, and we have recently expanded its remit and strengthened its role through the Justice and Security Act 2013. The Committee will undertake a detailed review and we would expect this to cover all aspects of this attack, including the issues you have raised and those relating to wider law enforcement and security agencies.

The Foreign Secretary and I believe that the ISC is the appropriate forum to consider these matters, and we are confident that its investigation will be comprehensive and robust. I hope you will appreciate that we are keen to avoid opening a dual track approach to Parliamentary scrutiny, or providing a running commentary which could prejudice what is an ongoing investigation likely to result in a criminal prosecution. On this basis we have decided to decline your request for this information.

I am copying this letter to Sir Malcolm Rifkind and Andrew Parker.

Rt Hon Theresa May MP
Home Secretary
June 2013

Written evidence submitted by the Home Office [CT 04b]
Letter from James Brokenshire MP, Security Minister, to the Chair of the Committee, 3 October 2013

Please find attached to this letter the Government's response to the Committee's call for evidence in respect of its inquiry into the Pursue strand of the Government's counter-terrorism strategy, CONTEST. Whilst I did not feel it appropriate to address each point in the inquiry's Terms of Reference, I have set out the Government's approach to *Pursue,* focusing in particular on *Pursue* delivery, counter-terrorism and security powers, countering terrorist finance and international co-operation.

A number of the inquiry's Terms of Reference cover areas which fall chiefly within the purview of the Intelligence and Security Committee (ISC); I have not, therefore considered these points in detail. Whilst there are clear parallels with Northern Ireland related terrorism in respect of the Government's approach, the CONTEST strategy focuses on tackling International Counter-Terrorism; as such, consideration of Northern Ireland related terrorism does not form part of this evidence.

JAMES BROKENSHIRE MP
Security Minister
3 October 2013

Evidence Submission: Home Affairs Select Committee Inquiry into *Pursue*

Introduction

1. The *Pursue* strand of the Government's counter-terrorism (CT) strategy CONTEST seeks to identify, investigate and disrupt terrorist attacks in this country and against our interests overseas, and - wherever possible - to prosecute those involved. This paper sets out in brief the key aspects of *Pursue,* considering the structures within which *Pursue* is delivered; the powers in place to target and disrupt terrorist activity; the roles of organisations such as the Charity Commission and Financial Conduct Agency in tackling terrorist financing; and the way in which the UK co-operates with other countries and multilateral organisations to counter the threat.

2. Recent events in Woolwich and the attack against the Westgate shopping mall in Nairobi, are a reminder that the threat the UK faces remains both serious and sustained and that the nature of that threat is evolving and diversifying.

3. The UK's record on CT remains a strong one. We continue successfully to disrupt attempted attacks against this country and its interests overseas. We are becoming more successful at prosecuting and convicting individuals engaging in terrorist activity. We delivered a safe and secure Olympic and Paralympic Games in 2012. And our CONTEST strategy, and the way we implement it, continue to be held up as examples of good practice around the world.

4. Key to this success is our commitment to continuous improvement: we regularly review our powers and capabilities to ensure they remain both effective and proportionate. A root-and-branch review of CT and security powers was an early priority for this Government and led to considerable reform; but monitoring and evaluation is an ongoing process. As we develop our powers and capabilities to meet new challenges, we will continue to ensure that we get the balance between security and civil liberties right. Recent events have led to some debate about the powers we have and the way we and our partners use them. Whilst it is not the

Government's policy to comment on intelligence matters or leaked material, the Committee will be aware that the Intelligence and Security Committee (ISC) has already published a report into allegations made by former US government employee Edward Snowden, which found that GCHQ acted entirely properly. In respect of the detention of David Miranda, we await the report of David Anderson QC, the Independent Reviewer of CT Legislation.

5. Despite our successes, there is no room for complacency: the threat continues to diversify both in terms of geography and methodology, and maintaining current levels of assurance will be challenging . Whilst we still face a significant threat from AI Qa'ida (AQ) in the border areas of Pakistan and Afghanistan, groups affiliated or associated with AQ have become stronger and more active across a range of unstable states, such as AI Qa'ida in the Arabian Peninsula in Yemen and AI Qa'ida in the Islamic Maghreb in West Africa. In Somalia, AI Shabaab remains capable of mounting attacks throughout the country and against targets in the wider region. The conflict in Syria has drawn extremists on both sides; whilst instability across that region has provided new ungoverned spaces for terrorists to operate in. Domestically,. there has been a trend towards 'low signature' terrorism by self-directed groups and lone actors. These individuals or groups develop the intent and capability to conduct attacks without support or direction from AQ or AQ-affiliates. Of similar concern· are 'self-starters' who radicalise themselves over the internet and plan attacks independently. Their attack methods tend to be simple, requiring little money or technical ability, but detecting and disrupting such threats is a significant challenge.

6. To put these words in context, there have been six foiled terrorist plots in Great Britain since April 2010[1]. Other terrorist incidents of note over this period include the attempted murder of an MP by a student in May 2010 and the discovery of printer cartridge bombs in transit at East Midlands airport in October 2010. However, attack plots represent just a small proportion of all terrorist activity in the UK, and they tend to develop in groups already involved in terrorist facilitation. Timely disruption of these groups has prevented further attack plans developing.

7. Between April 2010 and March 2013, 580 individuals were arrested in Great Britain for terrorism-related offences. The majority of arrests over this period (446) were categorised by the police as international terrorism[2] (77°(o), with 80 categorised as domestic terrorism (14%) and 9 as Northern Ireland related terrorism. The number of arrests has increased in each of the past two years. In the most recent year from April2012 to March 2013, the number of arrests increased by 21% to 249 from 206 in the previous year. The longer term trend is fairly stable: since 2002, there have been on average 210 arrests per year. It should be noted that the relatively small number of terrorism-related arrests each year means that proportionately large fluctuations in percentage terms are not uncommon.

8. Of the 580 arrested between April 2010 and March 2013, 241 (42%) were charged with an offence.[3] Of the total arrested, 98 (17%) were charged with a terrorism-related offence, of whom 35 (36%) were charged with preparation for terrorist acts (Terrorism Act 2006, section 5)[4]. This has led to 64 people being convicted of a terrorism-related offence so far[5]. Of these,

[1] 'Foiled plots' are defined as plots involving one or more individual engaged in attack planning of any form who have been arrested, charged and convicted of a terrorism-related offence within the stated time period. The figure includes all forms of terrorism in Great Britain, but excludes Northern Ireland Related Terrorism in Northern Ireland.

[2] The remainder were not categorised.

[3] In some instances, an individual arrested for terrorism-related offences may be charged with a non terrorism-related offence.

[4] Data refers to the principal charge for each individual and does not indicate where individuals are charged with multiple offences.

[5] Includes all those arrested between April 2010 and March 2013 who had been convicted of a terrorism related offence as of 10 July 201 3. Some individuals are still awaiting trial and so conviction data should. be interpreted with caution.

31 (48%) were convicted of preparation for terrorist acts (Terrorism Act 2006, section 5). Following a number of trials relating to the most recent foiled plots, 2012/13 saw a significant number of individuals (13) convicted of preparation for terrorist acts. Since current records began in September 2001 and March 2013, 64% of those charged with terrorism related offences have been convicted.

9. As the threat changes, we will continue to focus on improving our understanding of the threat picture and maintaining our ability to disrupt and detect terrorist plots. No strategy can be 1 00% effective in mitigating the threat, and the risk of a successful attack is always present. Recent tragic events here and abroad have only strengthened our resolve to do all we can to protect the public from those who would do us harm, and we will continue to monitor, develop and refine our powers and capabilities to ensure they remain both effective against - and proportionate to - the threat we face.

1. *Pursue* Structures

10. Ownership and governance of *Pursue* sit, like the rest of CONTEST, with the Office of Security and Counter-Terrorism (OSCT) in the Home Office, but a wide range of organisations and partners are responsible for contributing to the development and delivery of *Pursue* policy. Whilst the police and the security and intelligence agencies - the Security Service (MI5), Secret Intelligence Service (MI6) and Government Communication Headquarters (GCHQ) - are at the forefront of operational delivery, a number of other Whitehall departments and their agencies have important roles to play in *Pursue,* including the FCO, Cabinet Office, HM Treasury and HMRC, along with other bodies such as the Charity Commission and Financial Conduct Authority. Close co-operation and dialogue between these organisations, underpinned by common objectives and priorities, and effective information and intelligence sharing, form the basis of successful *Pursue* delivery.

11 . The work of the **security and intelligence agencies** falls mainly within the purview of the ISC. These organisations play an important role in delivering and supporting policy, judiciary and law enforcement partners alike in combating the terrorist threat. On the operational side, the most important of these is the police.

12. **Policing** is key to *Pursue* delivery in the UK, and whilst the Metropolitan Police Service (MPS) plays a leading role in Great Britain, CT policing is delivered by every police force in the country. The national Police CT Network comprises the Counter-Terrorism Command (S015) within the MPS; four Counter-Terrorism Units (CTUs) in the West Midlands, West Yorkshire, Greater Manchester and Thames Valley; and Counter-Terrorism Intelligence Units (CTIUs) in the East Midlands, South West and Eastern regions, and Wales and Scotland. Individual forces also have their own Special Branch capability or equivalent.

13. The police contribution to delivering CT is co-ordinated by an ACPO committee - the ACPO (TAM) Board - using authority delegated by the Chief Constables' Council; major CT investigations are co-ordinated across force boundaries by the Senior National Co-ordinator under a national agreement. Police activity is funded by dedicated CT grants, the level of which is based on advice from the police and the agencies. Funding for CT policing has been protected since 2010, maintaining core capabilities, and as announced in the recent Spending Round, it will continue to be ring-fenced until 2015-16. The intelligence agencies also received a 3.4% increase in their combined budget for 2015-16.

14. A key aspect of police *Pursue* work focuses on protective security at **ports and airports.** The National Border Targeting Centre uses advance passenger information to issue alerts to Special Branch officers at ports about subjects of interest travelling to and from the UK, and *to* deny airlines authority to carry to the UK individuals who pose a threat. These officers

investigate people and goods involved in terrorism to obtain intelligence, and make arrests where appropriate.

15. The creation of the **National Crime Agency** (NCA), which will be formally established in October 2013, represents a significant change to the policing landscape. The NCA will lead work on serious, organised and complex crime, including cyber crime and border security. Once the agency is up and running the Government will consider what - if any - role, it should play in respect of CT. Until then, the NCA will work with the Police CT Network on issues of. common interest.

16. Successful disruption and prosecution of terrorist suspects does not necessarily eliminate the risk they pose, meaning partners such as the **National Offender Management Service** (NOMS) are also vital to Pursue delivery. NOMS has a well-established intelligence infrastructure which identifies risk and threats within prisons, from evidence of attack planning to radicalisation and recruitment activity, and ensures that relevant intelligence is shared and jointly analysed with partner agencies and the police to disrupt extremist activity. This includes informing decisions about how and where high risk offenders are held, to developing appropriate interventions to tackle extremism and radicalisation within prisons.

2. Counter-Terrorism & Security Powers

Prosecution

17. The most effective way of dealing with terrorist suspects is to prosecute them and, in the case of foreign nationals, subsequently to deport them. Responsibility for prosecuting terrorism-related cases in Great Britain lies with the Special Crime and Counter-Terrorism Division of the Crown Prosecution Service (CPS). Suspected terrorists are prosecuted for 'ordinary' criminal offences as well as those provided for by specific CT legislation; many of those involved in serious terrorist activity are prosecuted for offences based on the wider legal framework, most notably offences such as conspiracy to murder. Last year, 43 people were charged with terrorism related offences in Great Britain, with 18 prosecuted and 16 convicted. A further 24 were awaiting trial on 31 December 2012, with 2 individuals having been acquitted. These figures represent a strong performance.

Disruption

18. While prosecution is always our preferred option, it is not always possible. The first priority must be to protect the public; as such, the police often need to take action to disrupt terrorist activity before they have been able to gather enough evidence for a prosecution. In other circumstances, a prosecution might not be practical because information against the suspect is not admissible in court due to . national security concerns - frequently, the need to protect our capabilities. For this reason, other means of disrupting terrorist activity are necessary to address the threat these individuals pose to public safety. Again, these measures are subject to robust safeguards to ensure they are effective, proportionate and consistent with our legal and human rights obligations. The main measures are as follows:

• ***Terrorism Prevention and Investigation Measures (TPIMs):*** Examined extensively by the Committee in the past, the TPIM regime restricts the ability of terrorist suspects to engage in terrorist-related activity, thus reducing the risk they pose to the public. In his 2012 report, David Anderson QC concluded that "so far TPIMS have been effective in preventing terrorist related activity".

• ***Exclusion:*** The Home Secretary has the power to exclude from the UK individuals from outside the European Economic Area (EEA) whose presence she does not consider 'conducive to the public good.' Since January 2005, 442 people have been excluded from the UK, including on grounds of national security (234) and unacceptable behaviour (extremism) (162).

• ***Deprivation of citizenship:*** Since 2006 over 20 individuals who posed a real national security threat to the UK have been deprived of their British citizenship and either prevented from returning to the UK or removed from this country. Deprivation of British citizenship results in simultaneous loss of the right of abode in the United Kingdom and so paves the way, for possible immigration detention, deportation or exclusion from the UK.
• ***Deportation with assurances (DWA):*** Deportation with assurances agreements are an important component of CT co-operation with international partners. They enable the UK to deport foreign nationals suspected of terrorist activity in compliance with its obligations under human rights law. DWA arrangements have been agreed with Jordan (to which the Government recently succeeded in deporting Abu Qatada), Lebanon, Algeria, Morocco, Ethiopia and Libya (not currently operational).
• ***Royal Prerogative:*** The Government's ability to stop individuals from travelling abroad to engage in terrorism-related activity has become increasingly important with recent developments in Syria and other places of concern. A range of measures are in place which can be used to disrupt such travel, which include the Home Secretary's Royal Prerogative power to refuse or withdraw a British passport on public interest grounds. This is an important tool to disrupt individuals who plan to engage in fighting, extremist activity or terrorist training overseas and then return to the UK with those skills. New powers to search for and seize passports cancelled by the Home Secretary under the Royal Prerogative, as well as other invalid travel documents, have been introduced into the Anti-Social Behaviour, Crime and Policing Bill.

Preventative Measures
19. As well as targeting individuals, an important element of *Pursue* is to disrupt the activities of terrorist groups, including their recruitment and funding activities.

• **Proscription** enables prosecution for membership and other activities in support of terrorist groups; it also shows solidarity with international partners. Proscription also facilitates other disruptions, including prosecutions and immigration disruptions such as exclusion. In July 2013 Boko Haram and Minbar Ansar Deen in Nigeria were proscribed, and the Al Nusrah Front in Syria was recognised as an alias of Al Qa'ida.
• Working through the UN and EU, the UK also uses targeted international **sanctions** against individuals and groups suspected of terrorist activity which can severely restrict their ability to operate. In July 2013, after a sustained period of UK lobbying, EU Foreign Ministers agreed to list Hizb'allah's military wing as a terrorist organisation; and in the first half of 2013, the UK worked with other Member States at the UN to ensure that the UN Al Qa'ida sanctions regime reflected the emerging terrorist threats in north and west Africa. The restrictive measures imposed by CT sanctions include travel bans, arms embargoes and asset freezes on designated individuals or entities.

Reviewing our powers
20. Ensuring our CT powers - and the legislation underpinning them – remain both effective and proportionate is a cornerstone of our strategy, one which reflects our commitment to protecting the people of this country and our interests overseas in a way which is consistent with British values, including transparency, human rights and the rule of law. The Government's review of CT and security powers, published in January 2011[6], made changes to the toolkit to make it more effective, targeted and proportionate.
• We concluded that **stop-and-search powers** under Section 44 of the TACT Terrorism Act 2000 must be repealed, and replaced them with a more limited power which enables the police to stop and search people and vehicles without reasonable suspicion only in exceptional circumstances where there is a real threat of terrorist attack.
• We also reduced the maximum period of **pre-charge detention** from 28 to 14 days - though recognising that in exceptional circumstances a temporary increase to a maximum of 28 days

[6] Available at https://www.gov.uk/governmenUpublications/review-of-counter-terrorism-and-securitypowers

might be necessary, an emergency Bill has been prepared as a contingency, subject to Parliament's approval.
• We also recently commenced **post-charge questioning** powers in Great Britain to enable terrorist suspects to be questioned after being charged – an additional investigative tool for the police and prosecutors where further evidence emerges after charges have been brought. The purpose is to allow prosecutors to build more robust evidential cases.

21. Evaluation of our powers is an ongoing process. **Schedule 7** of the Terrorism Act 2000 enables police officers to stop, question, detain and search people travelling through ports to determine whether they are or have been involved in terrorism. Schedule 7 confers an important CT power, but the Government recognises there are concerns about its use. We recently conducted an extensive public consultation on Schedule 7; amendments will be proposed in the Anti-Social Behaviour, Crime & Policing Bill, including reducing the maximum examination period to six hours.

22. Recognising the need to protect intelligence and the capabilities for gathering it, we also introduced the **Justice and Security Act,** which allows for closed material proceedings in the small number of civil cases involving national security sensitive material; and for judicial reviews of exclusion and deprivation decisions to be heard by the Special Immigration Appeals Commission (SIAC). These measures have equipped the courts better to handle sensitive material to serve the interests of both justice and national security, while allowing the Government to defend its case for the use of these executive actions, even where decisions are based fully or partly on material which cannot be disclosed in open court without damaging national security.

23. The Government also remains committed to ensuring that the law enforcement and intelligence agencies have the powers they need to investigate crime, protect the public and ensure our national security, including maintaining access to communications data. The Government's approach will be proportionate, with robust safeguards in place, but we cannot let cyberspace become a haven for criminals and terrorists.

3. Counter-Terrorist Finance

24. The need to tackle terrorist financing is an important aspect of *Pursue:* terrorists need money to organise and conduct attacks, maintain their networks, travel, and radicalise and train others. This is challenging: the amounts of money involved are often small and difficult to trace, and the means by which terrorists raise, move and store money are diverse, ranging from abuse of charity to exploiting weak regulatory environments to conducting kidnaps for ransom.

Banking & Money Service Businesses
25. Terrorists use banks and money service businesses (MSBs) to move and store funds; the **Financial Conduct Authority** (FCA) and **HMRC** are therefore key partners. The FCA supervises banks' compliance with the Money Laundering Regulations and focuses on ensuring that banks have robust systems and controls in place to prevent money laundering and highlight suspicious activity. HMRC supervises money service businesses under the same regulations; information relating to terrorism is passed to law enforcement agencies.

Financial Action Task Force (FATF)
26. Ensuring robust regulatory regimes in overseas jurisdictions is an important dimension in countering terrorist finance. The UK is a strong supporter and active member of the Financial Action Task Force (FATF), which sets international standards for legal, regulatory and operational measures to combat money laundering and terrorist finance. FATF conducts regular evaluations of countries' regimes and sets actions plans for those with deficiencies; high-risk jurisdictions which do not take steps to improve their regimes can be 'grey-listed' or

'black-listed' by FATF, which can limit investment and participation in international markets. This has produced tangible results: Kuwait has recently taken significant steps to improve its regime, including ratifying the Terrorist Finance Convention and enacting legislation; and both Kenya and Ethiopia have also introduced legislation due to FATF pressure.

Charities

27. The conviction in February 2013 of three individuals for raising money for terrorist purposes by posing as charity fundraisers, underlined the importance of the role of the Charity Commission, the charity regulator in England and Wales, in countering terrorism and extremism. Traditionally, the Commission has focused on regulatory monitoring and compliance. We have been working closely with the Commission and its new chair William Shawcross to look at how it can take a tougher line with those who seek to abuse the sector for terrorist purposes, including through more effective and targeted use of its existing powers against charities of CT concern. Where necessary we will seek to enhance those powers to improve the Commission's ability to regulate the sector as a whole.

28. Working with the Home Office, law enforcement and other partners, the Commission has already increased the number of compliance visits it conducts into charities of CT concern, both to identify and investigate abuse by terrorists and to improve awareness of and increase resilience to such abuse. As part of that awareness-raising the Commission has published guidance to the sector on stopping extremist speakers and monitoring charitable funds, including its successful 'Safer Giving' campaigns. More recently, it has run workshops on sending aid to Syria and other high risk areas. Internationally, we will continue to work with the Commission and other partners to improve its visibility of charities' activities - and of their financial footprints- overseas.

4. International Co-operation

Bilateral and Multilateral Engagement

29. Many threats to the UK involve an international dimension, and the diversification of the threat in recent years has made it ever more important that we work with a wide range of countries to disrupt the threat to the UK and to build capability to counter terrorism at source. We work in close co-operation on both policy and operational channels with our international counterparts in accordance with our values, the rule of law and our own legal obligations.

30. Our most developed CT relationships are with our '5 Eyes' partners: the US, Canada, Australia and New Zealand. We have unique intelligence relationships with these countries and hold regular, detailed exchanges of views on CT policy and strategy issues. We also have close relationships with European countries, both bilaterally and through the European Union. The UK is regarded as a source of expertise on CT within Europe, and we work closely with EU bodies (CT Coordinator, Commission, Europol, External Action Service) and other Member States to set the direction for European CT activity. The UK opt-out of Justice & Home Affairs measures will not restrict our ability to co-operate fully with other European countries to tackle terrorism. We are also engaged in agreeing priorities and action plans for the EU's external work, notably in building capability in the security and justice sectors in priority countries.

31 . The UK promotes greater international co-operation on CT through other multilateral forums such as the G8 and the Global Counter-Terrorism Forum (GCTF). This year's UK Presidency of the G8 focused on kidnap for ransom – achieving unequivocal rejection of the payment of terrorist ransoms - while the GCTF is developing its work in the areas of rule of law and criminal justice capacity building, including the establishment of an International Institute for Justice and the Rule of Law (opening in 2014), which will train legal practitioners to international standards.

Overseas Capacity-Building

32. In 2013, the Government introduced a more strategic approach to its efforts to develop the capacity of international partners to investigate and prosecute terrorists by building justice and human rights partnerships with countries where there is both a threat to UK security and weaknesses in the law enforcement, human rights and criminal justice architecture. Supported by a £30m CT Programme Fund, these partnerships include work to:
• Build the CT capacity of overseas security services to improve compliance with the law and human rights and to make them more effective;
• Improve the ability of local investigators to build cases based on evidence rather than confession. The police CT network plays a critical role in this regard: support is delivered through the network of Counter-Terrorism and Extremism Liaison Officers (CTELOs) posted overseas who work with organisations in their host countries and regions;
• Ensure prosecutors and judges are capable of processing terrorism cases through the court systems, effectively, fairly and in line with the rule of law;
• Improve and where appropriate monitor conditions in detention facilities so that convicted terrorists can be held securely and their treatment meets with international standards.

33. Safeguards have been designed to ensure that this work is carried out within a framework built on accountability and respect for human rights; it is vital that our CT work supports justice and the rule of law as well as meeting our security objectives. Although work on the partnerships is in its early stages, we have already delivered progress in a range of areas, including the establishment of focused CT prosecutor cadres in key countries, more effective handling of CT cases through the courts and improvements in CT investigators' evidence gathering and forensics skills.

Conclusion
34. The latest version of CONTEST considered what success in *Pursue* looked like: effective disruption of terrorist-related activity in the UK and more prosecutions or deportations of those responsible; reducing the threat from Al Qa'ida, its affiliates and other organisations overseas, including disrupting attacks planned against the UK; and ensuring that our CT work is effective, proportionate and consistent with our commitment to human rights.

35. Judged against these indicators, we are confident that our performance in delivering *Pursue* has been and continues to be strong. However, as the threat continues to diversify and originate from a wider geographical area, our ability to detect and disrupt potential plots will become ever more challenging. We cannot reduce the risk from terrorism to zero, but we will continue to work to disrupt those suspected of terrorist activity in the UK; to prosecute and convict them where we can; and where we cannot but they are foreign nationals, to take action to remove them from the UK. We do this by ensuring that our partners have a robust range of powers which enable them to do their job and their work is integrated and coordinated. We keep our powers and capabilities under regular review to ensure that they are effective and proportionate, and we are working ever more closely with overseas partners and organisations to improve both their and our capabilities to counter terrorism.

Written evidence submitted by the Home Office [CT 04c]

Letter from Charles Farr, Director General, Office for Security and Counter Terrorism, to the Chair of the Committee, 27 November 2013

QUESTIONS FOLLOWING HOME AFFAIRS SELECT COMMITTEE ON 12 NOVEMBER 2013

1. Thank you for your letter of 15 November 2013. As far as possible I have set out below the information you requested with additional information requested by Eleanor Scarnell on 18 November.

Mohammed Ahmed Mohamed case chronology

2. A case chronology of Mohammed Ahmed Mohamed including his Control Order and TPIM breaches is attached at Annex A.

Mohamed's civil claim for damages

3. Mohamed alleges that he was not detained in accordance with Somaliland law; that he was mistreated at the time of his arrest and when in detention; and that he was deported to the UK without due process. He claims the UK was unlawfully involved in this. As this matter is the subject of ongoing civil litigation I cannot comment on the issue at this stage beyond saying that the Government has denied any wrongdoing or unlawful acts.

TPIM breaches and prosecutions

4. Ms Scarnell asked for details of TPIM breaches and prosecutions. Six people have been charged with breaching their TPIM notices, some more than once:

Mohamed himself was charged on two separate occasions – in December 2012 with six counts of failing to report to the police station or reporting late (awaiting trial at time of abscond) and in July 2013 with one count of tampering with his tag (case discontinued after CPS concluded there was no realistic prospect of conviction). As noted in Annex A, he was also charged with 14 counts of breaching his Control Order.

One person pleaded guilty to three counts of breaching - broadcasting without permission, attending a meeting or gathering without permission and entering an internet cafe without permission. He was sentenced to nine months imprisonment on 21 June 2013. Charges in relation to a further three counts were allowed to lie on file following his guilty plea.

One person was charged with five counts of entering an excluded area without permission. The CPS discontinued the prosecution because, in their view, there was no realistic prospect of a conviction.

In three cases (of which Mohamed was one) charges relating to tampering with the electronic monitoring tag were discontinued after the CPS concluded that challenges to the reliability of the forensic evidence meant that, in their view, there was no realistic prospect of a conviction.

One person was found not guilty in relation to two counts of breaching - failure to report to the police station and failure to report to the monitoring company as required.

One person is currently remanded in custody awaiting trial, having been charged with one count of breaching - having an unauthorised meeting.

Control order absconds

5. You asked whether any of the control order absconds were connected with a mosque. One control order subject, who absconded in 2007, was last seen at a mosque. There is no evidence to indicate that any of the other six individuals subject to Control Orders absconded from mosques. One person is believed to have escaped from a window of West Middlesex Hospital; three who were not tagged, disappeared sometime after making a routine report to a police station; one who was tagged disconnected an electronic monitoring unit and cut off his tag at his home before disappearing; and one disappeared during the short window between one control order being quashed and a new control order being served against him on the same day. Control Order subjects did not have GPS tags. One of the purposes of the new tag is to provide reassurance of an individual's location and monitor his compliance with measures which restrict his movement.

Passports belonging to TPIM subjects

6. All the TPIM subjects are prohibited by their measures from possessing or taking any steps to obtain a passport. All passports of TPIM subjects, other than that of Mohamed, are accounted for and are in the possession of the police.

7. Mohamed was issued with a British passport on 28 April 2005. When he was deported to the UK he did not have this passport with him, so there was no passport for the police to seize. The whereabouts of this passport are unknown.

Mohamed's citizenship

8. Mohamed entered the UK, aged three, with his mother on 12 June 1989. His mother claimed asylum on her and her children's behalf on 29 July 1989. The family were recognised as refugees on 30 October 1989 and granted four years leave to remain. They applied for indefinite leave to remain on 20 September 1993, which was granted on 28 April 1994. Mohamed and his family were naturalised as British citizens on 23 November 1999, when he was aged 13. Under Somalia nationality law Mohamed automatically lost his Somali citizenship when he became British. He is therefore a UK mono-national.

Mohamed's deportation from Somaliland

9. As this matter is currently the subject of ongoing civil litigation I cannot provide any details further to what I told the Committee. However, I can confirm that documents relating to Mohamed's deportation from Somaliland were disclosed during open session in the TPIMs proceedings by both the Government and Mohamed's lawyers. These documents are not in the public domain.

10. You asked why Mohamed was allowed to return to the UK. Section 1(1) of the Immigration Act 1971 exempts from immigration control persons who have the right of abode. This means that there is no legal basis for preventing British citizens, like Mohamed, from returning to the UK, whatever the circumstances of their return and whatever their activities abroad. Where someone is a British citizen, it is not therefore necessary for a foreign government to request that we take them back.

Deportation of suspected terrorists to the UK

11. You asked about the number of people who have been detained overseas for terrorism offences, who were not prosecuted, and were then deported back to the UK. I cannot yet give you a definitive answer to this question. I have asked officials to work with the police and their network of Counter Terrorism and Extremism Liaison Officers (CTELOs) to collate the information which we expect to send you in early December.

The possible prosecution of TPIM subjects for terrorist offences

12. You asked whether Mohamed or other TPIM subjects could have been prosecuted were it not for sensitivities around evidence being produced in open court. For each TPIM case, under section 10 of the TPIM Act 2011, the CPS review all material held by the relevant agencies in order to determine whether there is evidence available that could realistically be used for the purposes of prosecuting the individual for an offence relating to terrorism. This review is, of course, conducted according to existing evidential rules and does not address a hypothetical situation where secret intelligence material could be used as evidence.

13. The CPS have told me that it is not possible to say, on a case-by-case basis, how such a hypothetical situation would affect the prospects of prosecution because the evidential rules that would apply in such a situation are, by definition, unknown. However, to help the Committee, I have asked the CPS to give their overall opinion of what difference the use of secret evidence might make to their ability to prosecute TPIM subjects. The CPS are considering this and I will write to you soon with the results. I would note in the meantime para 7.15 of David Anderson's 2012 TPIM report (published March 2013) which states: "I asked the CPS to tell me whether their decisions not to charge any of the 10 TPIM subjects would have been different had intercept evidence been admissible in criminal proceedings. Having consulted the relevant case lawyers, they advised me, without confirming whether or not such material existed in any case, that their charging decision would have remained the same in each of the 10 cases".

Communications data

14. You asked me to provide further data on the breakdown of requests for communications data, particularly with reference to GCHQ. This data is collected and collated by the Interception of Communications Commissioner.

15. The Commissioner's 2012 Annual Report stated that there had been 570,135 requests for data that year. It is not possible to identify accurately the number of people to which these requests relate. The reason for this is that at the time of an application for data and subsequently it is often not clear to law enforcement agencies how many people are using a single phone or indeed who the „owner" of it might be. Members of criminal gangs and terrorist groups do not own a single phone like the rest of us. Phones are frequently shared and then disposed of very quickly. As I said in the Committee session, the requests will therefore relate to a significantly lower number of investigations and people – some investigations involve many hundreds of requests, many relating to the same person. The Joint Committee on the Draft Communications Data Bill, which reported in December 2012 described (in appendix 4 to the report) a case where 500 applications were made for different types of data relating to just five people.

16. The Commissioner's report outlines that 99% of total requests come from law enforcement and the security agencies. This includes police forces across the UK, the Serious and Organised Crime Agency (now part of the National Crime Agency), HM Revenue and Customs, the former UK Border Agency and the intelligence agencies

(MI5, SIS and GCHQ). The remaining 1% relate to requests from other public authorities; the vast majority are from the Financial Services Authority (now the Financial Conduct Authority and the Prudential Regulation Authority) and local authorities.

17. The Joint Committee on the Draft Communications Data Bill recommended that more detailed information should be collated about communications data requests. The Home Office is keen to improve the public information on how communications data is used to support law enforcement investigations. We have consulted the Interception of Communications Commissioner on what additional statistics could be collected that would add value to his annual report to the Prime Minister. We are looking at a number of data categories such as the types of crime being investigated and the number of applications which are rejected (or where further work is required) at each stage of the process.

18. Please let me know if I can be of further assistance to the Committee.

Charles Farr, Director General,
Office for Security and Counter Terrorism
November 2013

Annex A

MOHAMMED AHMED MOHAMED – CASE CHRONOLOGY

On **5 May 1986** Mohamed was born in Somalia.

In **1989** Mohamed arrived in the UK.

On **23 November 1999** Mohamed was granted British citizenship (aged 13).

On **14 January 2011** Mohamed was arrested and interviewed in Burao, Somaliland with two other individuals. All three were accused of conspiracy to commit offences against national security. But Somaliland authorities did not prosecute any of the three because of insufficient admissible evidence. One individual was released locally; Mohamed and the third individual, a British national, were subsequently deported to the UK.

On **13 March 2011** Mohamed was deported back to the UK.

On **14 March 2011** Mohamed arrived in the UK. He was detained and examined under Schedule 7 of the Terrorism Act 2000. Following that he was served with a Control Order and relocated to a town in the east of England.

On **12 October 2011** Mohamed was arrested, and subsequently charged and remanded in custody in relation to **14** breaches of his control order:

18 August – failed to call monitoring company as required.

27 August – failed to report to police station as required.

7 September – failed to call monitoring company as required.

11 September – failed to report to police station as required.

15 September – failed to call monitoring company as required.

23 September – returned late for curfew.

28 September – met a person without prior permission.

28 September – possession of unauthorised mobile phone.

29 September – met a person without prior permission.

29 September – went outside his geographical boundary.

29 September – entered an internet cafe without permission.

30 September – failed to report to police station as required.

9 October – failed to call monitoring company as required.

11 October 2011 – unauthorised possession of an MP3 player.

On **21 February 2012** Mohamed was released on bail by the court after successfully arguing – amongst other reasons – that his trial for breaches should be delayed behind the High Court review of his control order. The CPS opposed bail but the Judge decided that, given the length of time Mohamed had spent on remand, bail should be granted. A TPIM notice was served on Mohamed the same day and he was moved to Home Office provided accommodation in London.

In **July 2012** the High Court heard the review of the lawfulness of the Control Order and TPIM.

On **19 October 2012** Lloyd Jones LJ handed down a judgment, upholding both the Control Order and TPIM.

On **29 December 2012** Mohamed was arrested, and subsequently charged and remanded in custody in relation to **six** breaches of his TPIM between 22 and 28 December 2013 (failing to report to the police station or reporting late).

On **19 April 2013** Mohamed was released on bail by the court (again, the CPS opposed bail). The High Court had upheld the control order and TPIM in a judgment handed down on 19 October 2012, but Mohamed argued that his trial for breach should be delayed behind his appeal against the High Court's judgment.

On **25 July 2013** Mohamed was arrested, and subsequently charged and remanded in custody in relation to **one** breach of his TPIM – a 'tag tamper' which occurred on 16 May 2013.

On **6 August 2013** – Mohamed was released on bail by the court (again, the CPS opposed bail). He continued to argue that his trial for breaches should be delayed behind his appeal against the High Court's judgment upholding the control order and TPIM.

On **1 November 2013** the CPS discontinued the prosecution for the alleged 'tag tamper' of 16 May 2013 because challenges to the reliability of the forensic evidence meant that, in their view, there was no realistic prospect of a conviction.
Later that day Mohamed absconded. His tag sent a tamper alert to the monitoring company, which was relayed by an automatic email to the Home Office and police. This was followed up by telephone between the monitoring company, Home Office and police. The Committee has received a confidential letter from G4S setting out further details of the immediate response, including precise timings. I can confirm the contents of that letter.

The police immediately launched an intensive operation to locate Mohamed. Ports and borders were notified with his photograph and details circulated nationally and internationally.

On **2 November 2013** the Court, on the application of the Home Secretary, lifted the anonymity order in place in relation to Mohamed.

On **3 November 2013** the police appealed for public's help in locating Mohamed.

At the point when he absconded, Mohamed was still on bail in relation to 14 breaches of his control order and six breaches of his TPIM notice. The court had listed a combined trial for these breaches for the week beginning 28 April 2014. If Mohamed is not apprehended it is likely that the trial will be postponed.

Mohamed's appeal against the High Court decision to uphold the Control Order and TPIM had been listed for hearing in January 2014. Discussions between the parties and the Court will now take place to decide whether the case should still go ahead

Written evidence submitted by the Home Office [CT 04d]

Letter from Charles Farr, Director General, Office for Security and Counter Terrorism, Home Office, to the Chair of the Committee, 16 December 2013

Suspected crimes committed by TPIM subjects

I am writing in response to a request from Eleanor Scarnell on 29 November for details of TPIM subjects who a) are believed to have committed a UK crime, but cannot be prosecuted for it; and b) are not believed to have committed a UK crime.

Before she can impose a TPIM notice, the Home Secretary must have reasonable belief that the person concerned is, or has been, involved in terrorism related activity (in the UK or overseas). In all of our TPIM cases this belief, which is lower than the criminal test, has been upheld by the courts. Involvement in terrorism related activity would, of course, almost certainly constitute a UK crime.

As required by Section 10 of the TPIM Act, before any TPIM notice is imposed, the Crown Prosecution Service reviews the evidence available and must advise the Chief Officer of Police that there is insufficient evidence to prosecute the person concerned for an offence relating to terrorism.

So to answer the question posed; all TPIM subjects are 'reasonably believed' to have been involved in terrorism related activity likely to constitute a UK crime for which they cannot be prosecuted.

Charles Farr, Director General,
Office for Security and Counter Terrorism
December 2013

Written evidence submitted by the Home Office [CT 04e]

Letter from Charles Farr, Director General, Office for Security and Counter Terrorism, to the Chair of the Committee, 6 January 2014

CONTEST

1. Thank you for your letter of 29 November asking the following further questions following my appearance before the Home Affairs Select Committee on 12 November.

Two years on from the 2011 review of CONTEST, are you satisfied that the planning assumptions upon which the strategy is based are still relevant?

2. I am satisfied that our planning assumptions in 2011 continue to be relevant. They do not mention Syria specifically though they do refer to the likely increase in activity by Al Qaida affiliates and their exploitation of instability in the Middle East. Syria of course reflects these broad trends.

Are Afghanistan, Pakistan, Yemen, Somalia and Nigeria still the priority countries for our counter-terrorism work overseas? What about Syria? What is the risk regarding the conflict in Syria?

3. Afghanistan, Pakistan, Yemen, Somalia and Nigeria remain priority countries for our counter-terrorism work overseas. Syria has also become a priority. We face the threat of a terrorist attack conducted against this country and our interests overseas from Syria based groups; these groups may make use of foreign fighters (including - but not only - people from this country); foreign fighters, particularly those returning to this country, may also pose a threat to us in their own right.

One assumption from the 2011 strategy is that there will continue to be isolated individuals who engage in terrorist activity in the name of extreme right or left-wing views but they will not present as high a risk as AQ. Is that still the case in light of the Pavlo Lapshyn case?

4. We believe this assumption remains valid.

Overseas Capacity Building

How many overseas capacity building projects are the UK involved with? Please provide us with a list of countries and a brief description of the purpose and activity of each of the projects with reference as to how they are funded i.e. fully by UK Govt or jointly between UK and EU, jointly between UK and US etc. Please give us a detailed case study of a capacity building project including its objectives and how its effectiveness would be measured.

5. We do not publicly disclose the location, number or purpose of all our counter terrorist capacity building projects overseas because they very often have a counter terrorist operational purpose. UK and third country personnel working in these projects may be at risk from terrorist groups.

6. Capacity building is coordinated by the Foreign and Commonwealth Office and concentrated in countries from where there is a terrorist threat to the UK or to UK

interests. In general these projects aim to strengthen the capacity of these countries to investigate, detain, prosecute and convict terrorists in a manner which meets our human rights obligations. Programmes are mainly funded from the FCO CT Programme Fund which in 2013/14 is £30m.

7. Many of the projects are part of the Government's Justice and Human Rights Partnership programme, which was announced on 14 February in a speech by the Foreign Secretary. I am aware that you have written separately to the Foreign Secretary about that programme in the context of your inquiry into counter-terrorism.

8. While you will understand that I cannot go into details of the programme, one example is the CAPRI (Counter-Terrorism Associated Prosecutorial Reform Initiative) programme in Pakistan, which aims to increase the number of terrorism convictions in Pakistan by developing an effective CT legislative framework and improving capacity within the CT criminal justice system, working with the Pakistani police, prosecutors and judiciary.

Foreign Fighters

Would the draft EU PNR directive improve our abilities to monitor those who we suspect to be foreign fighters and, if so, what work is the UK doing to ensure that the EU PNR directive is passed by the European Parliament?

9. The Justice and Home Affairs Council has made clear that tackling the issue of foreign fighters is a priority for the EU and we are working closely with our European partners and meeting frequently to discuss means of practical co-operation. The Government considers that PNR (including intra European PNR) and API can support work on foreign fighters and continues to lobby for PNR at the European Parliament.

How many UK foreign fighters in Syria are thought to have joined the al Qaeda linked groups Jabhat al Nusra and ISIS?

10. We believe that more than 200 UK-linked individuals have travelled to Syria to join the fighting.

To date, how many UK nationals/residents have returned to Britain after fighting in Syria?

11. Many people who have been to Syria have returned to this country. I am unable to provide details in this letter.

What actions have been undertaken by government agencies to identify returning foreign fighters?

12. This is an operational issue and you will understand that I am unable to provide any details. Doing so would clearly undermine our work to identify foreign fighter in future.

Has the Government developed a mechanism for assessing the risk posed by returning UK nationals who have participated in the Syrian civil war?

13. As you would expect it is a routine part of the counter terrorist work of the agencies and of JTAC to identify and assess all types of terrorist threat to this country, including the threat from people who have returned to the UK after fighting in Syria.

What are the government's plans for dealing with returning British foreign fighters?

14. You will understand why I am unable to provide specific details of all of the actions that are being taken for these purposes.

Communications Data

Has GCHQ collected communications data relating to communications between people within the UK, where such communication was routed outside the UK?

15. All data collected by GCHQ is acquired and handled lawfully, in accordance with the Regulation of Investigatory Powers Act 2000 and the Intelligence Services Act 1994. The Intelligence and Security Committee is briefed in detail on GCHQ's activities and capabilities and their legal basis and I am unable to provide any further detail in this letter. As I have stated in my evidence on 12 November GCHQ has never provided and can never provide the communications data necessary to address the communications data capability gap, for which the Government has proposed legislation

Court cases

In the past month we have seen the collapse of prosecutions against Mohammed Ahmed Mohamed and others and against Dr Shajul Islam and others due to the CPS not presenting a case. What are the barriers to presenting such cases and are you satisfied that the CPS have the capacity to prosecute trials such as these?

16. The CPS decided to discontinue the prosecution against Mohamed and two other TPIM subjects for suspected tag tampers because, in their view, challenges to the forensic evidence meant there was no realistic prospect of conviction. In the case against Dr Shajul Islam the prosecution was unable to call either victim to give evidence. Both of these decisions were based on the evidence available and CPS resources were not a factor.

Please could you send us an update regarding the CPS work on the attempt to stay Mr Mohamed's legal applications against the Government?

17. Mr Mohamed has two ongoing cases against the Government. The first is an appeal against his control order and TPIM notice, and the second is a civil damages claim. We continue to keep these cases under review. While his abscond is not in itself a ground to stay his litigation, Mr Mohamed is under an obligation to meet the requirements set by the court for pursuing that litigation and his lawyers may only act on his behalf as far as they have instructions. It is for the court to determine whether these requirements are met and ultimately, whether these cases should proceed. These are civil cases and are therefore not dealt with by the CPS.

Charles Farr, Director General,

Office for Security and Counter Terrorism

January 2014

Written evidence submitted by Professor Clive Walker [CT 05]

Introduction

1 This paper responds to the call on 23 July 2013 for evidence from the Home Affairs Committee on aspects of the 'Pursue' strand of the CONTEST strategy. This paper addresses just one element: 'Whether the Charities Commission has reduced the ability of terrorists to obtain funding through charitable donations.'

2 Discussion in this paper derives from my research over many years into anti-terrorism laws and also, more recently, into regulatory action and litigation involving charities suspected of financing terrorism. For fuller details and arguments, see principally:

- Walker, C., *Terrorism and the Law* (Oxford University Press, Oxford, 2011)
- Walker, C., 'Terrorism financing and the policing of charities: who pays the price?' in King, C. and Walker, C. (eds.), *Dirty Assets: Emerging Issues in the Regulation of Criminal and Terrorist Assets* (Ashgate, Farnham, 2014)

Background

3 Attention to the financing of terrorism has intensified since the attacks on September 11, 2001. Underlying characteristics within charities which give rise to vulnerability include enhanced public trust, diversity of financial activities, cash intensiveness, complex multiple donor patterns, and the involvement of politically committed individuals.

4 The potential link between charities and terrorism finance was signalled internationally by the Financial Action Task Force ('FATF') in October 2001, when it issued its Special Recommendation VIII on Terrorism Financing.[1] The FATF identifies three categories of charity abuse.[2] The first concerns the use of bogus charities as fronts for terrorists. The second is the fraudulent (or at least furtive) diversion of properly raised funds which are subverted towards terrorist purposes. The third example involves broader

1 These rules were revised in 2012: http://www.fatf-gafi.org/topics/fatfrecommendations/documents/ixspecialrecommendations.html. See further FATF, *International Best Practices: Combating the abuse of non-profit organisations - Special Recommendation VIII* (Paris: 2002).

2 FATF, *Terrorist Financing* (Paris: 2008) 10, 11.

exploitation of a charitable umbrella, such as through the recruitment and payment of extremists or for the propagation or glorification of a militant ideology. It is difficult to find clear examples in the United Kingdom within the first category. The second category will typically arouse suspicions about the humanitarian work abroad of cultural associations based within minority communities. The third category also presents some risk.

5 The risk of charitable funding of *jihadi* terrorism is viewed as affected by two further factors. One is the Islamic custom of *zakat* – the duty of donating personal wealth for charitable purposes. The second factor affects those charities which are active in regions of conflict (such as Afghanistan, Pakistan, Palestine, Somalia, and, hitherto, Sri Lanka). They are thereby especially vulnerable to the risks from working alongside protagonists within the conflict and by the limits or costs of formal banking systems requiring reliance upon informal remittance systems.

6 These depictions of the political and legal salience of contemporary terrorism finance and the centrality of charities in its operation underplay the personal (non-financial) commitment which drives terrorism and the personal integrity of charity workers who view their independence from terrorism and government as crucial to their work. The allegations of complicity in terrorism also overplay the analogy to criminal racketeering or more generally to rational choice theory. Terrorist operations are often inexpensive, especially for the late modern (dis)organisation of many *jihadi* groups, and do not start with the motive of amassing personal wealth.

7 So far as the United Kingdom law is concerned, legislation against the funding of terrorism is a core part of 'CONTEST'[3] and is executed by the Terrorism Act 2000, Part III, as supplemented by Anti-Terrorism, Crime and Security Act 2001, Part I, the Counter-Terrorism Act 2008, Part V, and the Terrorist Asset-Freezing etc. Act 2010. This submission will first briefly explain these policing mechanisms. The findings will lead into analysis of the key questions: 'do they work' and, if so, 'who pays the price' of the policing and regulatory burdens?

[3] See Home Office, *Countering International Terrorism* (London: Cm 6888, 2006), as updated by (London: Cm 7547, 2009; Cm 7833, 2010; Cm 8123, 2011; Cm 8583, 2013).

Policing and regulatory mechanisms applied to charities

8 Whether within the 'policing' or 'regulation' of charities, there are the following essential elements of activity: the specification of rules or standards; the monitoring of compliance; and the establishment of enforcement devices. These elements are reflected at two policing levels: 'internal' and 'external'.

Internal policing

9 Internal policing applied to charities demands that they should monitor their own business and procedures to ensure that terrorism financing does not take place. A number of specialist measures comprise this watchfulness against terrorism financing.

10 First, trustees of charities, like everyone else, must not to withhold information about terrorism, breach of which is a criminal offence (section 38B(2) of the Terrorism Act 2000). A more onerous duty along the same lines is imposed by section 19(1) of the Terrorism Act 2000. When a person believes or suspects that another person has committed an offence under either of sections 15 to 18 on the basis of information accruing in the course of a trade, profession, business, or employment, an offence is committed if the information is not disclosed to a police officer or member of the Serious Organised Crime Agency ('SOCA') or even the Charity Commission as soon as reasonably practicable. In the drafting of section 19, the government emphasised the confinement of the onerous duty to professionals. However, the reach of section 19 has been significantly supplemented by the Counter-Terrorism Act 2008, section 77, arising from allegations that charities were being misused for terrorism financing[4] and that trustees did not pay sufficient attention – thus, in 2006, just 48 Suspicious Activity Reports (SARs) were issued from the charitable sector, a dearth of suspicion which officialdom found 'hard to explain'.[5] Section 77 inserts, as section 22A of the Terrorism Act 2000, a new definition of ‘employment’ which encompasses both paid and unpaid

4 See HM Treasury, *The Financial Challenge to Crime and Terrorism* (London: 2007); Home Office and HM Treasury, *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse* (London: 2007).

5 Home Office and HM Treasury, *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse* (London: 2007) paras 3.3, 3.6. The impact of SARs is debated: House of Lords European Union Committee, *Money Laundering and the Financing of Terrorism* HL 132 (2008–09) and HL 11 (2010-11).

employment and can even include voluntary work. In this way, unpaid volunteers who are the trustees of a charity must act with the same insight as professional forensic accountants.

11 An even stricter duty to disclose is imposed on the 'regulated sector'[6] by Schedule 2, Part III, of the Anti-Terrorism, Crime and Security Act 2001. Under section 21A (inserted into the Terrorism Act 2000), a person in that sector commits an offence by knowing or suspecting or having reasonable grounds for knowing or suspecting, that another person has attempted or committed an offence under either of sections 15 to 18 (including with extra-territorial effect), unless that information is disclosed to a constable, officer of SOCA, or the employer's nominated officer as soon as practicable. The duty is subject to a reasonable excuse not to disclose. The objective standard of liability, which can arise without subjective awareness of any suspicion, is justified by the '[g]reater awareness and higher standards of reporting in the financial sector'.[7] Charities do not generally fall within the 'regulated sector', but the financial institutions which handle their transactions certainly do so. For instance, the Royal Bank of Scotland was fined £5.6m (including a 30% discount for early settlement) by the Financial Services Authority in 2010 for failing to ensure funds were not transferred to people or organisations on sanctions lists, leading to an 'unacceptable risk' of facilitating terrorist financing.[8] More serious criticisms and regulatory penalties[9] and civil litigation have also been encountered by UK financial institutions in the United States, arising from the alleged defaults of United Kingdom banks in respect of accounts held by charities.[10]

External policing

12 External policing is principally exerted by the Charity Commission, under Part II of the Charities Act 2011. In the context of alleged links to terrorism, there may be two triggers for investigation. One is that the charity is overstepping the boundaries of its charitable status

6 Terrorism Act 2000, Sch 3A, as substituted by: Terrorism Act 2000 (Business in the Regulated Sector and Supervisory Authorities) Order 2007, SI 2007/3288; Terrorism Act 2000 and Proceeds of Crime Act 2002 (Amendment) Regulations 2007, SI 2007/3398.

7 Home Office, *Regulatory Impact Assessment: Terrorist Property* (London: 2001) para 8.

8 <http://www.fsa.gov.uk/pubs/other/rbs_group.pdf >.

9 See US Senate Permanent Sub-Committee on Investigations, *US Vulnerability to Money Laundering, Drugs and Terrorist Financing* (Washington DC: 2012). HSBC paid a fine of $1.92bn.

10 See *Weiss v National Westminster Bank* 2008 US Dist LEXIS 99443 (EDNY), (2013 U.S. Dist. LEXIS 52628, USDC EDNY, 28 March 2013).

by supporting political purposes which are espoused by terrorist groups.[11] This first potential problem has not been the prime issue. Instead, the allegation is commonly that money is being used to fund activities which are in part political or social but also in part violent.

13 The enforcement powers of the Charity Commission, in sections 76 to 87 of the Charities Act 2011, are sweeping[12] but rarely used[13] and are in practice circumscribed by two limitations. The first is that while charities with a turnover above a specified amount (of £5,000) must register under section 30 of the Charities Act 2011, there is no obligation to adopt the form of a charity by not-for-profit bodies. Some groups are suspicious of potential meddling or do not recognise any benefit in registration. For example, despite the efforts of the Faith and Social Cohesion Unit set up in 2007, a minority of the estimated 1,672 mosques in the United Kingdom are registered.[14]

14 The second limitation is that policing and enforcement are secondary in the constitution and culture of the Charity Commission. The Mission of the Charity Commission involves 'enabling', 'encouraging', and 'promoting',[15] while its statutory objectives in section 14 of the Charities Act 2011 comprise legal compliance by charity trustees with their legal obligations as just one objective amongst several. Likewise, the 'general functions' of the Commission in section 15(1)(3), without mention of any punitive or prohibitory sanction, refer to 'Identifying and investigating apparent misconduct or mismanagement in the administration of charities and taking remedial or protective action in connection with misconduct or mismanagement in the administration of charities.' The 'green-light' approach of the Charity Commission can be further evidenced by its six general duties in section 16 of the Charities Act 2011. General Duty 2 states that 'So far as is reasonably practicable, the

11 See Charity Commission, *Speaking Out - Campaigning and Political Activity by Charities* (London: CC9, 2008).

12 Home Office and HM Treasury, *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse* (London: 2007) para 3.

13 See *Charities Back on Track 2011-12: Themes and lessons from the Charity Commission's investigations and regulatory casework* (London: 2012) p 32.

14 Compare <http://www.muslimsinbritain.org/resources/masjid_report.pdf> ; Charity Commission, *Survey of Mosques in England and Wales* (London: 2009) p 5, and *Annual Report 2009/10* HC 77 (2010-11) 7.

15 *Annual Report 2009/10* HC 77 (2010-11) 22.

Charity Commission must act in a way which is compatible with the encouragement of (a) all forms of charitable giving, and (b) voluntary participation in charity work.' Furthermore, in performing all its functions, the Commission is required by General Duty 4 to 'have regard to the principles of best regulatory practice (including the principles under which regulatory activities should be proportionate, accountable, consistent, transparent and targeted only at cases in which action is needed).' In this way, the Commission constitutes a 'green-light' regulator rather than a 'red-light' regulator.[16] Because of this approach, more formal policing agencies find it hard to take over investigations started by the Charity Commission.[17] The claim that the Charity Commission is hobbled, in part by the framing of law and in part as a self-induced restraining organisational culture, may be next tested by some case studies.

The application of external policing

Regulatory responses

15 If a charity becomes designated under the international sanctions regimes, the need for regulatory action is palpable. But designation has only affected two charities operating in the United Kingdom jurisdiction. Assuming a charity is not internationally designated, then regulatory action is much less straightforward. The version of 'green-light' regulation thesis adopted here is not that the Charity Commission wholly ignores allegations of terrorism. Its caseload of 180 investigations in 2009-10 included 11 which related to allegations or suspicions of terrorist-related activities.[18] Rather, the issue is whether its resolve to deal with the allegations is sufficiently firm. Three cases might be highlighted. These are selected as more recent than the notorious case of Abu Hamza's involvement in the North London Central Mosque (Finsbury Park), more straightforward than the various inquiries into Interpal, the facts about which are disputed, and less affected by media pressures (as applied to the handling of Viva Palestina).

16 One case concerned the Ikhlas Foundation, which was registered in 1997 and whose main work involved the 'Muslim Prisoner Support Group' and especially related to prisoners

[16] The terms are adapted from C. Harlow and R. Rawlings, *Law and Administration* (Cambridge: 3rd ed, Cambridge University Press, 2009) chap 1.

[17] Home Office and HM Treasury, *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse* (London: 2007) para 3.20.

[18] Home Office, *Prevent Strategy* Cm 8092 (2011) para 10.196.

impugned for involvement in terrorism. The group had been of serial concern to the Charity Commission because of the activities of various trustees.[19] In 2007, Mohammed al-Ghabra, a trustee, was removed after he was designated by the UN and by the HM Treasury in December 2006.[20] The Charity Commission was apparently unaware of this designation until informed in July 2007; he was removed as a trustee in October 2007. However, no sanction was imposed on the remaining trustees even though the Commission viewed them as inadequately recognising or managing the risks. Instead, the inquiry was closed on the commitment by remaining trustees to strengthen their governance within three months. That undertaking by the trustees did not bear fruit. A second inquiry began in 2008, when another trustee, Abbas Taj, was suspended by the Commission (and later resigned) following his arrest in 2008 and conviction in 2009 for conspiring in an arson attack on a publisher. The Commission recorded that the trustees had failed to deliver on their previous commitments.[21] Despite this recurrently woeful record, the Commission concluded its second inquiry by issuing a direction under section 19A by which the trustees were set a further few months to regularise their meetings and membership, to conduct a risk assessment, and to mitigate risks. Given that the charity had a very modest income of around £5,000 per annum, the risk of terrorism financing should not be exaggerated. Nevertheless, the patience of the Charity Commission accorded to this serially delinquent charity was astonishing, though the Ikhlas Foundation has since been removed from the Register of Charities.

17 The second case, Iqra, a bookshop and learning centre in Beeston, Leeds, registered as a charity in 2003. Its activities came to an abrupt halt in 2005, when it was confirmed that two of the July 7 bombers, Mohammed Siddique Khan and Shehzad Tanweer, had acted as trustees. The police raided its premises, as a result of which the remaining trustees claimed that the charity had become inoperative. Another trustee, Khalid Kaliq was subsequently convicted of terrorist-related offences not directly related to Iqra. Yet, not until 2009 did the Charity Commission decide to launch a formal inquiry, and even that step seems to have been prompted by media reports. In the event, the Commission found no evidence that Iqra's finances or premises had been used for the preparation of the July 7 attacks, and it can hardly be blamed for not detecting terrorist connections more astutely than the police or security

19 Charity Commission, *Inquiry Reports: The Ikhlas Foundation* (London: 2008 and 2010).

20 See *HM Treasury v al-Ghabra* [2010] UKSC 2 at [1].

21 Charity Commission, *Inquiry Report: The Ikhlas Foundation* (London: 2010) paras 38, 39.

agencies. However, the Commission found that extremist materials had been possessed and also admitted that no action had been taken over the fact that no reports or accounts had ever been filed by the trustees. Awakening from this stupor after further prodding by the media, the Commission took steps to seize the remaining trust money (£12,500). [22]

18 The third example concerns the charity, Sivayogam,[23] an organisation which worked with Tamils both in London and in northern Sri Lanka. Concerns surfaced in 2005 when it became public that the leading trustee, Nagendram Seevaratnam, had professed LTTE sympathies. The Inquiry instigated by the Charity Commission found problems with the selection and monitoring of local partners in Sri Lanka, with financial accounting, and with the involvement of a trustee who remained openly supportive of the LTTE. In another example of its 'green-light' style, the Charity Commission imposed the sanction of removal of one trustee but otherwise sought to work with the impugned charity to improve its standards. Even the attempted removal was reversed by the First-Tier Tribunal (Charity), which viewed the trustee's statements as merely 'unwise and unguarded'[24] and that contact with the LTTE did not make it necessary or desirable to remove him.[25] Furthermore, the Tribunal endorsed a 'green-light' regulatory approach:[26] 'If there had remained any legitimate regulatory concerns following a proper examination of the evidence originally provided to it, the Tribunal concludes that it would have been appropriate for the Respondent to work with the charity to improve its processes before considering exercising its regulatory powers.'

Assessment of responses

19 This track record of the Charity Commission does not match the seriousness with which the threat of terrorism is depicted in CONTEST. That verdict is subject to two provisos. One is that further efforts have been instituted since 2006 to improve the relevant guidance. The second point is that there are competing public interests which may legitimately affect the degree and manner of intervention by regulators. These two provisos will now be considered.

22 Charity Commission, *Inquiry Report: Iqra* (London: 2011).

23 Charity Commission, *Inquiry Report: Sivayogam* (London: 2010).

24 *Nagendram Seevaratnam v Charity Commission for England and Wales and Her Majesty's Attorney General* (CA/2008/0001, 13 October 2009) para 6.52.

25 *Ibid*, paras 6.93, 6.117

26 *Ibid*, para 6.75.

20 In response to the evident perils of terrorist abuse and infiltration of charities, the Home Office and HM Treasury reviewed the policing regime in their 2007 report, *Review of Safeguards to Protect the Charitable Sector (England and Wales) from Terrorist Abuse*'.[27] The government departments urged the Charity Commission to reinforce its guidance, and it responded in 2008 by publishing its *Counter-Terrorism Strategy* wherein it promised 'zero tolerance'.[28] In pursuance of its strategy, various actions have been undertaken to improve trustee awareness, including oversight through a Proactive Monitoring Unit, cooperation between enforcement agencies, and greater intervention. Published advice has been further elaborated through the issuance of an *Operational Guidance* and a *Compliance Toolkit*, setting out the Commission's approach, and underlining the duties of vigilance and disclosure of trustees, illustrating the possible threats, and giving advice about the work of the Counter Terrorism Team which forms part of the Intensive Casework Unit in Compliance and Support.[29] The *Compliance Toolkits* were impressively expanded in 2013.[30]

21 Despite these documentary elaborations, there has been no discernible change in the 'green-light' approach. The Home Office commented in its 2011 paper on *Prevent Strategy*[31] as part of the 'Next Steps' agenda that 'The Charity Commission must be seen to be capable of taking robust and vigorous action against charities that are involved in terrorist activity or have links to terrorist organisations.' The accompanying independent survey by Lord Carlile is more candidly critical of the Commission.[32] This analysis of the continuing attitude and approach of the Charity Commission tallies with some recommendations in the report by Lord Hodgson in 2012, *Trusted and independent: giving charity back to charities - review of the Charities Act 2006*.[33] Lord Hodgson not only calls for automatic trustee disqualification

27 (London: 2007) para 2.10.

28 (London: 2008) 4, 10.

29 Charity Commission, *OG96: Charities and Terrorism* (London: 2007); Charity Commission, *Compliance Toolkit: protecting charities from harm* (London: 2011).

30 <http://www.charitycommission.gov.uk/detailed-guidance/protecting-your-charity/protecting-charities-from-harm-compliance-toolkit/>.

31 Home Office, *Prevent Strategy* Cm 8092 (2011) para 10.203.

32 Lord Carlile, *Report to the Home Secretary of Independent Oversight of Prevent Review and Strategy* (London: Home Office, 2011) paras 58, 60.

33 (London: Cabinet Office, 2012). See also *Response to the Charities Act review from the Minister for Civil Society* (Cabinet Office, 2012).

following any conviction of a terrorism offence[34] (which would not make much difference) but also that the Charity Commission should take 'a more robust approach to potentially failing organisations' and 'proactive as well as reactive steps' in cases of abuse.[35]

22 Moving next to the competing public goods, these countervailing considerations are that British society should not appear to be stone-hearted in the face of humanitarian crises in conflict zones, such as in Palestine, Somalia, and Sri Lanka. Such a stance might even aggravate the situation by encouraging less regulated and less cooperative activities, even resulting in a strategic defeat. An illustration of such upheaval arises from the United Nations listing of the Al Barakaat group in Somalia from 2001 to 2009.[36] However, another public good is the punishment of wrongdoing which, in this case, may curtail the financing of terrorism and uphold the integrity of the charitable sector.

Future regulation

23 The United Kingdom approach to charities assailed by the taint of terrorism funding has been one of considerate understanding if not, at times, excessive 'green-light' leniency. Equally, their bankers are rarely at risk except in US civil courts. Thus, worthy individuals pay the highest price for relief work at the margins of legality. The Charity Commission is wholly correct to be highly suspicious of self-serving allegations from the opponents of Palestinians, Tamils, and other oppressed peoples and to adopt a stance which is primarily encouraging of compliance with high standards of governance rather than a condemnatory approach. But its serial indulgence of patent abuses does not aid the charitable sector.

24 Two facile reactions should be avoided. One would be to swing entirely towards criminal prosecution and asset forfeiture, a stance which would unduly ignore competing public goods. The second mistake would be to seek to reinforce the punitive resolve of the Charity Commission. The data from this chapter suggests that the Commission's weak statutory remit and entrenched 'enabling' culture cannot easily be nudged. A more promising

34 *Ibid.*, para 4.53.

35 *Ibid.*, para 4.29, 5.28.

36 M Scheinin, *Reports of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism* (A/HRC/6/17, 2007) para 48.

third way is to emphasise the value of financial investigation to facilitate intelligence-gathering. Prosecution and confiscation remain possible outcomes but should be less pressing than disruption and the gathering and transmission of data about terrorism activities other than just financing.

25 A financial investigation approach could have produced outcomes of greater utility to counter-terrorism in several of the inquiries described in this paper. It would have been more likely to have delivered information about terrorism networks and to close off the facilitation of militancy, but without hurting worthy causes. This financial investigation approach is not best placed in the hands of the Charity Commission but should primarily be conducted by a formal police body. The roles left for the Charity Commission would be as standard-setter, as standard-monitor (with early alerts back to the police financial investigators), and as standard-applier (with police advice). In this way, the heaviest price for terrorism financing should be paid by professional profit-takers and recipient perpetrators of terrorism.

Professor Clive Walker
Centre for Criminal Justice Studies
School of Law
University of Leeds
September 2013

Written evidence submitted by Professor Sir David Omand GCB [CT 06]

Any review of the Pursue strand of the UK Counter-Terrorism strategy CONTEST should start with the underlying logic of the strategy: the application of risk management to achieve the aim of the strategy, maintaining conditions of normality.

It is important in assessing the past and current effectiveness of Pursue to see it as a means of managing, not eliminating, the risk from terrorism. Elimination of risk from terrorism, and from AQ associated groups specifically, is most unlikely to be feasible over the next 5 years (CONTEST originally had a timespan of five years, that has been extended twice after review by successive governments). And attempts to achieve the absolute aim of eliminating terrorism would undoubtedly have highly undesirable side effects on the liberties and freedoms and respect for human rights that we rightly prize as British values.

In constructing the CONTEST strategy after 9/11, we saw the overall level of risk faced by the public from international terrorism as the product of a number of factors:

(a) the likelihood of attack (to be reduced both by the immediate Pursuit campaign to uncover and disrupt terrorist networks with a doubling of the capacity of the Security Service supported in increases in police and other intelligence effort, and by the longer term Prevent campaign aimed at countering the radicalization of another generation of young violent extremists at home and abroad);

(b) the level of vulnerability of the nation to terrorism (to be reduced by the Protect campaign improving security for aviation and the travelling public, crowded spaces and the critical national infrastructure);

(c) the size of impact of an attack, should (when) terrorists manage to penetrate our defences, together with the duration of the ensuing disruption to normal life (to be reduced by the Prepare campaign through improving emergency services and first responders capability and building resilience so as to enable the nation to bounce back as quickly as possible after attack).

It takes a balance of investment in all 4 Ps (Pursue, Prevent, Protect and Prepare) materially to reduce the overall risk, and although Pursue is fundamental it is a part of a larger strategy (with interaction between the Ps, for example taking care that over-vigorous Pursuit activities overseas do not prejudice the efforts of Prevent in our towns and cities).

That underlying risk management logic remains, has stood the test of time and should be re-endorsed.

When I decided to launch work to construct CONTEST in October 2002 we were unsure what should be the ultimate aim to which all those involved in the UK counter-terrorism effort, directly and indirectly, should bend their efforts. For the United States, suffering from the aftermath of 9/11, the overriding goal was to defeat terrorism and

> "use every tool available to disrupt, dismantle, and destroy their capacity to conduct acts of terror. The final element to the Defeat goal is an aggressive, offensive strategy to eliminate capabilities that allow terrorists to exist and operate - attacking their sanctuaries; leadership; command, control, and communications; material support; and finances".[1]

After much debate, we concluded on the other hand that whilst sharing that absolute determination to protect the public, for the UK the appropriate strategy should start from denying the terrorists that which they most sought, namely the creation of conditions of insecurity and fear amongst the public. The strategic aim of CONTEST – to reduce the risk in order to be able to maintain normality - has remained constant since then, from its acceptance as government strategy in 2003 to date. Formally:

> "The aim of CONTEST is to reduce the risk to the UK and its interests overseas from terrorism, so that people can go about their lives freely and with confidence."[2]

The caveats 'freely' and 'with confidence' that we added are, however, very important especially when it comes to the Pursue strand.

By 'freely' should mean without having to sacrifice the values and liberties of a free democratic society. Further tuning of counter-terrorism powers in the light of experience and of shifts in the modus operandi of terrorist groups must be expected, such as has already happened with TPIMS, stop and search powers and reducing the length of time for which people can be held before charge for terrorist offences to 14 days. But further changes should be at the margins, since

[1] George W. Bush administration, *National Strategy for Combating Terrorism*, Washington DC: White House, 2003.
[2] HM Government, CONTEST: The UK's Counter-Terrorism Strategy, London: HMSO, July 2011.

the fundamental approach to UK CT legislation is sound in relation to the likely trajectory of the threat over the next few years. Improved miniaturisation and reliability of the relevant technologies may, however, make it easier remotely to monitor the whereabouts and communications of tagged convicted terrorist offenders released on licence in the community, an issue that will increase in salience as more of those guilty of terrorism related offences come to the end of their terms of imprisonment.

The caveat 'with confidence' is also important. We can see the nation enjoying national security when there is maintenance of trust in the ability of the authorities to enable normal life to continue, that is, with an absence of fear of attack, with markets stable, inward investment flourishing, international travel safeguarded, overseas visitors arriving and welcomed and so on.

By the fundamental standard of that aim the CONTEST strategy is succeeding, as was well demonstrated by the safe and secure Olympic Games last year. I see no reason to alter the aim.

The success of Pursue (and equivalent efforts by allies and partners overseas) has been not only in disrupting networks in the UK and their links overseas (including a significant number of major plots that have been well reported in the media), but also making it much harder for violent jihadists to operate in the UK without detection. The effect has, as the Committee has recognised, been a shift in the UK from large-scale plots that require long term planning, organisation (including support from trained jihadists overseas) and finance to smaller, cruder local attacks.

It should be borne in mind, however, that such a mutation in the threat could quickly reverse if the pressure was taken off, and if jihadists were to regain the initiative in havens overseas such as Yemen, and as al-Shabaab threatens in Somalia. The AQ printer cartridge plot out of Yemen uncovered at Luton airport showed how terrorists far afield can threaten our security. It must also be remembered that an increased threat of individual acts of violence increases the difficulty of the demands on the intelligence and security services to forestall attacks whilst still avoiding oppressive and counter-productive surveillance of the community as a whole. And as the aftermath of the Woolwich murder showed the authorities also need to be able to stifle provocations from the extreme right that could threaten to undermine harmony in our town and cities..

Such developments in the terrorist threat will intensify the tension between nations that unilaterally defend their interests with military means - including by targeted killing and in future by offensive use of cyberspace – and those who seek collective security under international human rights law. A current

example is the use of international humanitarian law to justify lethal US armed UAV attacks outside a recognised battle-space on those regarded by their past or current hostile terrorist activity as having foregone their non-combatant immunity. Other nations such as the UK will be seeking to defend themselves within the different legal construct of international human rights law, authorising lethal force only when hostile intent is actually being shown. We will see more examples of overlapping legal regimes operating in a single geographical space as nations try to protect their interests against terrorist and criminal movements in ungoverned spaces overseas. The Committee will, I am sure, consider the ethically ambiguous position of the British public that has benefitted in that respect from the US armed UAV programme that has removed several leading terrorists who had been associated with plans to attack the UK and UK interests, measures that would not legally be permitted to the UK under the overseas part of the Pursue strategy.

Terrorists will also adapt their methods to minimise the risk of failure. In the future the biggest change in the conflict environment may well be in cyberspace, given our increasing dependence on cyber systems and the connectivity provided already by 8 billion users of mobile devices, and this may make it more likely that violence is expressed against us from a safe distance lowering the risks to the attackers and lowering their threshold of violence.

Applying the principle of subsidiarity, security issues that can be handled locally should be: there is no need for the concept of national security to become unnecessarily centralised. Personal security, in the sense of absence of fear in one's home or workplace or when travelling, has traditionally been seen as a matter for local police services. These services, for example, play an important part in everyday preventive policing relevant to the success of both the Pursue and the Prevent strands, something that needs to be recognised by the new Policing and Crime Commissioners at a time when policing resources are under huge strain.

Especially since 9/11, however, it has become increasingly clear that important aspects of personal security are now national policy issues, because they have international roots in the activities of terrorists that see themselves as sharing a global religious ideology. There is thus a continuing need for a strong national counter-terrorism strategy to direct and align efforts supported by effective national intelligence and police capability working in harmony. The recent transfer of policy responsibility for the subject of serious and organised crime within the Home Office to OSCT to sit alongside counter-terrorism policy is prudent, given that we may see increasing overlap, or at least links, between criminal and terrorist gangs and that will include issues such as countering terrorist financing and terrorist access to cyber hacking capabilities. One

consequence of the spread of cyber attack capabilities is that no longer can the international community impose sanctions (such as the UN sanctions on Iran) and not expect the nation concerned to fight back with cyber means either directly or by proxies. Another is that commercial companies overseas will find themselves the subject of cyber or other form of attack (for example after an environmental disaster or simply because they represent Western 'Crusader' capitalism). It will be important that OSCT, with the agencies involved, looks broadly at how such hostile long term developments can be countered under a future Pursue strategy.

Does that also argue for transferring the responsibility for police leadership in counter-terrorism from the Metropolitan Police Service (the Met) to the National Crime Agency (NCA)? One of the great successes of the last decade for the UK has been the partnership between the police service and the intelligence and security community, and their relationship with the Crown Prosecution Service, something with which that most nations struggle. This fortunate position rests on established relations of trust between different organisations that have, rightly, different powers, mandates and cultures. That cooperation has been successfully tested in circumstances of terrorist attack and attempted attack, and in the successful conviction of terrorists in the Courts. Of course, the present arrangements involving the Security Service and the Met and the other police services in England and Wales and Scotland are not the only possible ones, nor necessarily the most economical. But they have evolved under fire and I would be very cautious about seeking to replace them with a theoretical structure that might look tidier on paper, such as giving the lead to the NCA, until we have seen both a significant diminution in the threat and an NCA that has established itself firmly as being on the top of its game in relation to serious organised criminality.

Furthermore, given the serious counter-terrorist effort still required in the UK, I would see great advantage in an all party statement from the Committee that the NCA should be given at least 5 years to bed down before the topic of counter-terrorism responsibility is reconsidered. What would erode unity of purpose and divert valuable nervous energy from the Pursue CT mission would be for officers on all sides to feel uncertain about the structure and their place in it over the next few years.

The purpose of Pursue is to stop terrorist attacks in this country and against our interest overseas. This means detecting and investigating threats at the earliest possible stage and disrupting terrorist activity before it can endanger the public and, wherever possible, prosecuting those responsible. The key to Pursue therefore is pre-emptive intelligence, soundly assessed.

Such intelligence can come from three sources: volunteered from the community; accessed from intelligence sources, including traditional and new secret sources (such as social media intelligence); and acquired from overseas liaisons. Although intelligence oversight is the province of the Parliamentary Intelligence and Security Committee, the Home Affairs Committee may wish to reaffirm the importance of all three of these avenues for accessing pre-emptive intelligence to allow terrorists to be identified, networks and attacks to be disrupted and those responsible for criminal acts brought to justice.

Looking ahead, it will be essential to an effective Pursuit campaign for the authorities to be able to continue to access and analyse stored communications meta-data and thus uncover the communications of terrorist suspects and their backers and financiers, even when these are hidden in the vast global volumes of the internet. Following the controversy over revelations by Mr Snowden of details of the capabilities of the US and UK intelligence communities to achieve precisely that there is the danger that well-meaning but exaggerated concerns over privacy, international information sharing and the effectiveness of oversight will hinder the future ability to track terrorists at home at abroad. The Pursue effort would be seriously undermined by misguided efforts to rush in new European or national regulation or by failure by Parliament to keep up to date UK legislation on internet communications data.

It is likewise important to Pursue that the detailed sources and methods of intelligence work and of investigations by police and Security Service do not become known to the terrorists themselves thus making their ambitions to harm us much easier to achieve. The proceedings of relevant criminal and civil cases have already revealed much of how the security authorities operate, and judicial proceedings in this country - civil as well as criminal - must be such as to be able to handle sensitive and secret material to preserve the interests of national security whilst dispensing justice.

The spread of existing and developing technology will create dangers, for example with ever more sophisticated IEDs drawing on mobile phone and shaped charge technology, improvised communications networks being used by terrorists (as seen in the Mumbai attack), and improvised weapons systems where current conflicts already provide a reservoir of weapons, including surface to air missile systems as well as a training and hardening experience for British jihadists who are likely to seek to import their new skills into domestic terrorism. The protection of UK and Western interests overseas, such as in aviation, oil and extractive industries, may well become more difficult, as was seen in the attack earlier this year by a 30 strong armed AQIM jihadist group on the BP/Statoil natural gas facility at In Amenas in south eastern Algeria near the Libyan border.

Another long term factor that should be considered when examining the future of the Pursue strand is that most of the additional global population growth that experts predict will end up in the overcrowded urban littoral of developing nations. The capacity of these urban mega-cities will be greatly exceeded in terms of security, governance, and basic utilities such as water and sanitation. In the vast slums of coastal urban sprawl will hide terrorists, religious fanatics, and violent criminal and pirate gangs with international connections to the West including in the UK. Safeguarding UK and Western interests and citizens, and when necessary organising rescue and evacuation, is likely to be a preoccupation of military and security planners.

What will be very different in future is that all of these many hundreds of millions of people living on the margin will nevertheless be electronically interconnected by their mobile devices, exposed to ideologies hostile to us and aware of global events as they happen. The implications for counter-terrorism strategy and the Pursuit of terrorists will be profound. There should therefore be no let up in the work by HMG to co-operate with governments overseas and international organisations to improve global responses to terrorism at source whenever it appears.

It is the international dimension of our major security risks that drives the need for a redefinition of national security. The increased vulnerability of advanced cyber-networked societies and reliance upon complex just in time global logistic networks and product sourcing widens the boundary of everyday security. Interdependent markets, global travel patterns and labour migration interacting with transnational terrorism and piracy all internationalise domestic security concerns. Success in counter-terrorism therefore depends on international collaboration including with countries whose legal outlook and respect for human rights differ from our own. That should not stop us standing up for our values, whilst encouraging and supporting key partners to build up their capacity to investigate and prosecute terrorists overseas.

Professor Sir David Omand GCB
War Studies Department King's College London
September 2013

Written evidence submitted by Chairman Peter T King [CT 07]

In response to the Home Affairs Committee's ongoing inquiry into the United Kingdom's counter-tenor efforts, I write to encourage the Committee to examine programs that help identify individuals attempting to travel abroad to join al Qaeda and wage jihad. As recent events have demonstrated, one of the most significant challenges facing Western states in the fight against al Qaeda is stemming the flow of foreign fighters who attempt to fight alongside al Qaeda's affiliates in Syria, Somalia, Yemen, and other parts of the world.

On August 22, 2013, then-Director of the United States Federal Bureau of Investigation (FBI) Robert C. Mueller publicly reported that citizens of the United States had travelled to Syria to fight with rebel groups attempting to overthrow the Assad regime.[1] It is also no secret that many of the factions fighting in Syria are allied with al Qaeda. In fact, one of the largest and most lethal rebel groups, the al-Nusra Front, is officially considered a terrorist organization by both the British and American governments, as well as the United Nations (U.N.), and is widely considered anal Qaeda affiliate.

This presents a threat to every country fighting violent Islamist extremists. The danger is exemplified by the several incidents of British and American citizens charged with ties to terrorist groups acting in Syria over the past year. An American woman from Flint, Michigan was killed while fighting in Syria in May.[2] In February, a British man died battling the Assad regime as a member of a group of Sunni extremist foreign fighters.[3] Video of his group, the Katiba al-Muhajireen (the Battalion of the Migrants), released in June shows individuals from several European countries, as well as Canada and the United States fighting Assad's forces near western Aleppo.[4] They are only one of the many armed groups allied with al Qaeda's Islamic State of Iraq and al Nusra Front wings.[5]

The security vacuum within Syria and the relative ease with which individuals can cross the Syrian border makes it difficult to track the movements of jihadi fighters or determine their exact numbers and identities. This problem is compounded by the fact that, according to British Foreign Secretary William Hague, "there is enough uncontested space in Syria for some violent Islamist groups to provide extensive training. This is particularly concerning as we assess some of the individuals being trained will seek to carry out attacks against Western interests in the region or in Western states, now or in the future."[6] The Chairman of the U.S. House of Representatives Permanent Select

1 "FBI Director: Some US Citizens Fighting in Syria Could Pose Threat in Future," ABC News Videos, Yahoo News, August 22, 2013. (Available at: http://news.yahoo.com/video/fbi-director-us-citizens-fighting-002845294.html)

2 "Flint woman, 33, killed by Syrian government forces, family says," Niraj Warikoo, the Detroit Free Press, May 31, 2013. (Available at: http://www.freep.com/article/20130530/NEWS06/305300146/Flint-woman-killed-in-Syria)

3 "First British fighter killed in Syria named as Ibrahim al-Mazwagi," Oliver Duggan, The Independent, March 03, 2013. (Available at: http://www.independent.co.uk/news/world/middle-east/first-british-fighter-killed-in-syria-named-as-ibrahim-al mazwagi-8518517.html)

4 "Britons fighting with Syria's jihadi 'band of brothers'," Sasha Joelle Achilli, Channel 4 News, June 14, 2013. (Available at: http://www.channel4.com/news/syria-war-rebels-jihadi-ibrahim-al-mazwagi)

5 "Rebels Gain Control of Government Air Base in Syria," Anne Barnard and Hwaida Saad, the New York Times, August 5, 2013. (Available at: http://www.nytimes.com/2013/08/06/world/middleeastlrebels-gain-control-ofgovernment-air-base- in-syria. html?smid=tw-share& _r= I &)

6 "Committee questions Foreign Secretary on Syria," Foreign Affairs Committee, UK Parliament, April 24, 2013. (Available at: http://www.parliament.uk/business/committees/committees-a-z/commons-selectlforeign-affairscommittee/news/fs-syria-response/)

Committee on Intelligence (of which I am a member) has also acknowledged that, "at some point all of these people from Europe are going home. All the folks there from all over the world, including the United States, will be coming home if they do not meet their end on the battlefield."[7]

As Chairman of Committee on Homeland Security in the U.S. House of Representatives during the 112th Congress, I held a series of hearings to examine the danger of homegrown Islamist extremists in the United States. My Committee found that dozens of Americans have travelled abroad to join al Qaeda to fight and train in multiple spots around the globe. Not only did these individuals in some cases attempt to return to the United States, but many became leaders within al Qaeda in their own right – gaining a reputation on the battlefield as was the case with Omar Hammami in Somalia, or using their knowledge of Western society to spread al Qaeda's message like Anwar al-Awlaki.

While we can only estimate, most experts suggest that the number of foreign fighters allied with al Qaeda's groups in Syria is a significant figure. Many report there are at least several hundred overall, with perhaps as many as 100 British citizens linking-up with primarily al Qaeda-backed groups.[8] For the United States, the figure is slightly smaller.[9] According to one report from July of this year, there are now more Westerners in Syria than there have been in other conflicts involving al Qaeda-linked extremist groups in Iraq, Afghanistan, Somalia or Yemen.[10]

It appears that most foreigners hoping to join the jihad in Syria move south into the country from Turkey. According to the United States Congressional Research Service (CRS), most foreign fighters prefer travel via Turkey (and northern Lebanon) because of "better regional air-travel linkages with Beirut and Turkish cities."[11] In fact, one international airport in Adana, Turkey has international flights to multiple destinations in Germany, and sits only a few hours drive from the Syrian border near Aleppo.

As was demonstrated recently in Kenya, where individuals from several Western countries, including Americans and Britons, reportedly took part in an al Shabaab assault on a major shopping mall in Nairobi, this is a pressing challenge. Combatting it will require a joint, sophisticated effort on the part of countries such as the United Kingdom and United States. A solution demands a strategy to counter extremism that identifies the threat that violent Islamist extremism poses; coordination between national intelligence and law enforcement agencies and local law enforcement; proactive assistance from local communities most susceptible to radicalization and recruitment by al Qaeda; intelligence sharing and assistance among foreign pa1tners; and rigorous oversight to ensure regular evaluation and constant improvement. Therefore, as your Committee carries out this

7 "Americans Join Syrian Jihad, Sparking U.S. Intelligence Fears," Eli Lake, *The Daily Beast*, September 12, 201 3. (Available at: http://www. thedailybeast.com/ articles/20 13/09/ 12/americans-join-syrian-j ihad-sparking-u-s-intelligencefears. html)

8 "British fighters in Syria: Will they come home to roost?" *The Economist*, May 4, 20 13. (Available at: http://www.economist. com/news/britai n/2 1577081-government-worried-about-british-j ihadists-syriawith-reason-willthey-come-home)

9 Lake, *supra* note, 7.

10 ·"Worries Mount as Syria Lures West's Muslims," Eric Schmitt, *the New York Times*, July 27, 2013. (Available at: http://www .nytimes. corn/20 13/07 /28/world/middleeastworries-mount -as-syria-1 ures-westsmuslims. html?page\vanted=all)

11 "Armed Conflict in Syria: Background and U.S. Response," Jeremy M. Sharp, Christopher M. Blanchard, *the Congressional Research Service*, September 6, 201 3. (Available at: http :1/crs.gov/pages/Reports.aspx?PRO DCO D E=R L3 348 7 & Source=search)

investigation, I encourage you to further study how best to prevent the citizens of ours and other countries from travelling to fight with al Qaeda, and how we can track and prosecute those that do.

Furthermore, the willingness to travel to terror safe havens and join violent Islamist extremist groups, even when these attempts are unsuccessful, should be considered an indicator that these individuals are capable of carrying out attacks in their home countries, as in the case of the Woolwich attackers, one of who reportedly attempted to join al Shabaab in 2010, and in the case of Tamerlan Tsarnaev.[12] Some reports suggest that Tsarnaev's travel to Russia in early 2012 was an attempt to meet with violent extremists in the Caucuses.[13] Both of these individuals would return home and subsequently murder innocent victims in the name of jihad.

My colleagues and I in the United States Congress are grateful our country has reliable partners and good friends in the United Kingdom. We eagerly await the results of your investigation, because the questions the Home Affairs Committee is attempting to answer are of vital importance to the U.S., as well as to the U.K.

Please, do not hesitate to let my office know if we can be of any further assistance to your effort.

Chairman Peter T king
Member of Congress
September 2013

12 ·'Woolwich attack: suspects were known to security services,'· Rosa Silvem1an, *the Telegraph,* May 23, 20 13. (Available at: http://www. telegraph. co. uklnews/uknews/terrorism-in-the-uk/1 00 7 623 9/W oo lwich-attack -suspects-wereknown-
to-security-services.html)

13 ·'Dagestan lslamists Were Uneasy Abo ut Boston Bombing Suspect," Alan Cull ison, *the Wall Street Journal,* May 9, 20 13. (Available at: http://online.wsj.com/article/SB I 000 1424127887324059704578473 1608661 08832. html)

Written evidence submitted by Tom Keatinge [CT 08]

1 AUTHOR AND SUBMISSION INTRODUCTION

1.1 Tom Keatinge is a near 20-year veteran of the banking industry who recently[1] studied for a Masters at King's College London which included a dissertation considering the effectiveness of the global 'Financial War on Terror' and the consequences of the counter-terrorist financing (CTF) regime that has been implemented since 9/11. He was also the banking contributor to a report commissioned during the summer of 2013 by DfID in light of Barclays Bank's decision to terminate bank accounts for a number of UK-based Money Service Businesses (MSBs).

1.2 As a result of this professional and academic experience, this submission focuses on the financial services industry (FSI) and associated regulatory elements of the inquiry's Terms of Reference.

1.3 The author is writing in a personal capacity and in no way represents any organisation with which he has previously been or is currently involved. The expressed views are thus strictly his own.

2 BACKGROUND

2.1 At the heart of the ongoing 'Financial War on Terror' is the Financial Action Task Force (FATF), set up by the G7 in 1989 and initially mandated to co-ordinate the global effort to counter the laundering of the financial proceeds of the drugs' trade. The UK is an active member of the FATF, contributing at all levels and leading many of its initiatives (e.g. the current work being undertaken to review the FATF's typology guidance for non-profit organisations, known as 'Recommendation 8').

2.2 Following 9/11, as the international community urgently sought to boost the global CTF regime, it seemed logical to extend the FATF mandate to include terrorist-financing.

2.3 Although not a legislative body, the implications of a country being designated 'non-compliant' by the FATF and included on its black-list are such that its guidelines have the same effect as regulations and are blindly implemented by many countries as they fear being cut off from the global financial community for failing to comply. The FATF is thus the *de-facto* global CTF regulator, a power that should not be underestimated.

2.4 In implementing the guidelines mandated by the FATF, countries primarily target two groups of operators: the financial services industry (FSI) and charities and other non-profit/non-governmental organisations (NPOs).

2.5 This submission argues that the effectiveness of this targeting has generally raised standards and awareness but is no longer 'fit for purpose' and needs to be radically rethought on both a UK national and global basis for three primary reasons, all of which are of importance to the Committee and its inquiry:

2.5.1 The FSI is expected to comply with ever widening and deepening CTF regulatory requirements with little or no intelligent or intelligence guidance from the authorities – banks and other financial service providers are effectively expected to play a counter-terrorist role with almost no meaningful assistance from the authorities.

2.5.2 NPOs are often stigmatised as a 'weak link' by those implementing CTF regulation leading to an increase in financial exclusion, entirely counter to the efforts of a number of global organisations to *increase* financial inclusion given the demonstrably positive development impact of such a policy.

2.5.3 MSBs, whilst undoubtedly able to improve compliance and due diligence standards, play an important role in moving money to regions where banks do not operate and thus, like NPOs, assisting with humanitarian and financial inclusion efforts. CTF regulation has led banks such as Barclays to the entirely understandable decision to close many MSB accounts given the pressures of the ever-mounting CTF compliance regime. Provision of such accounts and servicing 'high risk' regions is entirely uneconomic in light of the potential downside financial and reputational risk of being found to be (often unwittingly) non-compliant with CTF regulations.[2]

2.6 The global CTF effort is at an important juncture and the UK is a key participant in this effort. The easy tasks – improving standards in willing countries and at willing corporations – have largely been achieved, but vulnerabilities remain, and new ones are emerging as terrorist threats evolve. The global CTF regime has not adapted to reflect these changes and continues to waste time and resources 'on countering threats of the past.'[3]

2.7 Policymakers need to rethink why we have a CTF strategy, what are the precise goals of this strategy, and how these goals are being benchmarked and measured. If these goals are not being achieved they should have the courage to modify, replace, or scrap them.

2.8 It appears that since the initial urgency that 'something must be done' to target terrorist-financing in the immediate aftermath of 9/11, strategy in this arena has at best stagnated, and at worst continued down a sub-optimal path – significant reassessment is needed as the current policy is in many ways counterproductive.

2.9 Inflicting unnecessary cost and burden on corporations and nations, and restricting well-intentioned access to financial services, leading to greater use of the informal and black economies is not the way CTF will play an effective role in the counter-terrorist strategy of the UK or in international security, in fact, quite the reverse.[4]

3 REGULATORS, GOVERNMENT, AND THE FINANCIAL SERVICES INDUSTRY

3.1 Evidence suggests that there is a material disconnect between the expectations of regulatory and security authorities and the results delivered by the FSI.

3.2 Identifying terrorists' finances within a financial institution is extremely challenging. Flows are normally 'clean' and small (in contrast to the 'dirty' money laundered from the proceeds of crime).[5] In his 2012 testimony before the US House Committee on Homeland Security, Dennis M. Lormel who at the time of 9/11 was the Chief of the FBI's Counter-Terrorist Financing Operations Section noted that 'It is possible to identify terrorist financing, but highly improbable,'[6] and despite the immense amount of regulation developed in the context of CTF and the significant expense incurred by the FSI in terms of time, increased headcount, and systems upgrades, an extremely limited amount of terrorist financing has been revealed within the FSI.

3.3 It could thus either be the case that the regulations and requirements imposed on the FSI are not 'fit for purpose' or that the FSI is not used by terrorists to manage and move their financing.

3.4 Neither assertion is likely to be entirely right, rather it seems more probable that the FSI is not appropriately equipped to play the frontline role against terrorist financing that is demanded of it, primarily due to the almost complete absence of intelligence/security dialogue between the government/security authorities and the FSI, except when a specific threat has been identified.

3.5 Compliance with CTF requirements is a financial balancing act for the FSI, a judgment between blind compliance with whatever regulations are published through fear of the reputational and financial damage caused by exposure as non-compliant, and the considerable and increasing cost[7] of implementing AML/CTF regulation.[8] As noted by former US Assistant Secretary for Terrorist-Financing Juan Zarate, 'there has been an enormous burden placed on financial and commercial actors since 9/11'.[9]

3.6 The current regime results in the FSI doing whatever is necessary to meet its regulatory requirements in an almost entirely unguided manner. Thus, much of the action taken in this field by the FSI as a result of these pressures may be viewed as excessively conservative (for example closing MSB accounts) but given there is little co-operative interaction between the FSI and authorities in this arena, conservatism of operation is the best form of protection.

3.7 For example, the Committee will be familiar with the concept of a Suspicious Activity Report – the FSI is often incentivised to file SARs by quantity rather than quality given the lack of guidance and specificity from the authorities on *what* to look for.[10]

3.8 Furthermore, given the significant growth in the volume of SARs filed, it is highly questionable as to whether the authorities have the necessary numbers of staff to undertake real-time reviews of SARs that are submitted.

3.9 The resources of the FSI are considerable and if intelligently harnessed by regulators and security authorities could be of considerable financial intelligence value. The current situation is at best a missed opportunity and at worst a national security weakness.

3.10 *Recommendation: HMG must develop processes and systems by which it can interact more efficiently and effectively with the FSI to identify terrorist financing, providing feedback that allows the FSI to fine tune its considerable 'Financial Intelligence' gathering capability.*[11]

4 A POSSIBLE PARALLEL THAT COULD LEAD TO A SOLUTION MODEL

4.1 Earlier this year, HMG announced plans to establish a Cyber Security Information Sharing Partnership (CISP).

4.2 Comments made by Francis Maude at the Chatham House launch seem to offer a structure that could also be applied to enhance the effectiveness of the CTF regime in the UK. In particular he highlighted[12] that 'CISP is all about: Government and industry working together to build a comprehensive picture of the cyber threat and coming up with the best defences' noting that 'The private sector...is the most important line of defence...' and that 'the Prime Minister [had] held an event...for senior executives, to underline the benefits of a real and meaningful partnership between industry and government.' He further noted that 'The government's proposal was this: by building a community of public and private partners, we could all pool our information on cyber threats and increase our visibility of cyber threats for mutual benefit.'

4.3 Most succinct and directly applicable to the current lack of partnership between regulatory/security authorities and the FSI was his conclusion: 'This kind of working is the future: government and industry working hand-in-hand to fight a common threat.'

4.4 *Recommendation: The kind of partnership that CISP is developing should be considered as a model for a public/private partnership between government/security authorities and the FSI.*

5 MSBs, NPOs, and Financial Inclusion

5.1 Space does not permit a detailed review of the challenges posed to NPOs and MSBs by CTF regulation, and other responses and sources are available that cover this topic in detail.[13]

5.2 However given the global initiative to increase financial inclusion and the UK's role in this matter via, for example, the Prime Minister's co-chairing of the *High-Level Panel of Eminent Persons on the Post-2015 Development Agenda* which identifies access to financial services as a core requirement of the goal to 'Create Jobs, Sustainable Livelihoods, and Equitable Growth'[14] it is important to consider the impact that CTF has on this effort.

5.3 The continual and dramatic tightening of global AML/CTF standards and the resulting withdrawal by banks of many financial services deemed too risky (or not sufficiently profitable to justify the perceived risk) will inevitably have negative, unintended consequences on financial inclusion as MSBs and NPOs lose access to the financial services they need to move money to where it is most needed and the FSI both in the UK and developing world exclude organisations and individuals from the financial system on CTF grounds.

5.4 The FATF itself notes that '…applying an overly cautious approach to AML/CFT safeguards can have the unintended consequence of excluding legitimate businesses and consumers from the financial system,'[15] a side-effect that is particularly prevalent in high-risk and fragile state environments such as Somalia.

5.5 According to the World Bank, 'three quarters of the world's poor do not have a bank account, not only because of poverty, but [also] the cost, travel distance and amount of paper work involved in opening an account.'[16] For many of these 2.5 billion people, informal mechanisms such as MSBs play an important role, in particular as a means for delivering investment to hard-to-reach places along with much-needed assistance through Diaspora remittances.

5.6 Research undertaken by the World Bank and the Consultative Group to assist the Poor (CGAP) reach important conclusions with regards to the interaction between the provision of financial services to the poorer sectors of society and the establishment of an effective AML/CTF regime, noting that these objectives are 'complementary' as 'without a sufficient measure of financial inclusion, a country's AML/CTF system will safeguard the integrity of only [the formal] part of its financial system...leaving the informal and unregistered components vulnerable to abuse.'[17]

5.7 Broadening financial inclusion should be seen as a key and desirable element of establishing an effective AML/CTF policy and thus steps taken by the FSI and authorities that exclude users from the financial system and make the use of the underground economy seem more attractive are counterproductive.[18]

5.8 Somalia and the decision by Barclays to close a range of MSB bank accounts is a case in point. On balance, the creation of greater financial inclusion is likely to benefit security rather than detract from it. Often, no formal, viable financial link exists to connect families in fragile and post-conflict states with their overseas, Diaspora-based sources of money, thus restricting the flow of payments to these families leaves open a vacuum that can be filled by assistance from local terrorist organisations such as al-Shabaab, leading to increased support for the organisations that the international security community are trying to restrict via CTF measures.

5.9 Global regulatory authorities must therefore monitor closely whether the counter-terrorism measures they promote support or undermine security.

5.10 Recommendation: HMG needs to consider carefully the ways in which CTF measures lead to unintended negative consequences for financial inclusion, particularly with regards to the operations of MSBs and NPOs. A number of well researched studies demonstrate that there is significant scope for the implementation of CTF regimes to have a material impact on the humanitarian sector and financial inclusion.[19] A concerted, apolitical effort should be made to address the dilemma of facilitating the fast, efficient and cost-effective flow of finance to the poorest people in the world, while fighting terrorism. The status quo is often entirely counterproductive.

6 SUMMARY

6.1 In the case of both the relationship between regulatory/security authorities and the FSI and the impact of the CTF regime on financial inclusion and humanitarian efforts, there is too much focus on inputs (i.e. slavish adherence to the growing mountain of regulation) and not enough pause to consider the outputs of these actions. Credible and objective analysis of the effectiveness of the CTF regime needs to be undertaken to inform policy and decision-making – this is lacking and thus policies that may once have been well-intentioned have continued unchecked with generally little, or worse still, negative consequences.

6.2 Entrenched positions and a lack of meaningful and solutions-orientated dialogue mean that an element of counter-terrorism policy that has the ability to play an important role in UK national and international security has actually become at best simply an expensive, bureaucratic, wasteful, and redundant use of time and resources, and at worst an inadvertent impediment to the UK's counter-terrorist effort.

7 END NOTES

[1] MA in Intelligence & International Security completed in the War Studies Department of King's College London achieving an overall distinction and awarded programme prize for highest dissertation grade
[2] See, for example, the recent Financial Times article by Patrick Jenkins reflecting on HSBC's activities one year on from its US$1.9 billion fine from the US Government http://www.ft.com/cms/s/0/a175f712-1eea-11e3-b80b-00144feab7de.html#axzz2g6R6HSyX (accessed 28 Sept 2013)
[3] Biersteker, Thomas J. & Sue E. Eckert (2008) *Countering the Financing of Terrorism* (New York: Routledge), p.294
[4] Much of the research for this submission was gathered during the author's dissertation work in May-August 2012
[5] For example, according to the FATF (2008), the 7/7 bombings are estimated to have cost a mere GBP8,000 http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf (accessed 28 Sept 2013)
[6] Lormel, Dennis M (2012) Testimony to the US House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Lormel.pdf (accessed 28 Sept 2013)
[7] According to KPMG, this cost rose 45 per cent between 2008 and 2011. KPMG (2011) *Global Anti-Money Laundering Survey 2011: How Banks are Facing Up to the Challenge*, p.12
[8] It should be acknowledged that cases such as that involving HSBC in 2012 and the recently revealed activities of Liberty Reserve highlight the need for appropriate systems and monitoring at financial institutions – they are certainly not blameless
[9] Zarate, Juan (2009) *Smart Financial Power and International Security: Reflections on the Evolution of the Global Anti-Money Laundering and Counterterrorist Financing Regime Since 9/11* (Center for Strategic & International Studies)
[10] Interviews revealed cases where senior compliance managers of large banks were queried as to why such large banks were filing so few SARs: quantity seems to be favoured over quality
[11] Such processes must be consistent with the UK's data protection and privacy laws as well as relevant EU laws and directives
[12] Francis Maude (2013) https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme (accessed 28 Sept 2013)
[13] For example, DfID commissioned two reports over the summer of 2013 to consider the impact of Barclays Bank's MSB account closure decisions that included concrete proposals on how to improve and enhance the UK remittance market. These reports were discussed at a cross-Whitehall/industry roundtable on 27 September 2013
[14] Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda (2013) *A New Global Partnership: Eradicate Poverty and Transform Economies Through Sustainable Development* http://www.un.org/sg/management/pdf/HLP_P2015_Report.pdf (accessed 28 Sept 2013)
[15] FATF (2013) *Anti-money laundering and terrorist financing measures and financial inclusion* http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf, p.5 (accessed 28 Sept 2013)
[16] World Bank (2012) *Three Quarters of The World's Poor Are "Unbanked"* http://go.worldbank.org/61TLX5WSP0 (accessed 28 Sept 2013)
[17] Bester, H., D. Chamberlain, L. De Koker, C. Hougaard, R. Short, A. Smith & R. Walker (2008) *Implementing FATF Standards in Developing Countries and Financial Inclusion: Findings and Guidelines*, The FIRST Initiative (The World Bank, Washington, DC) (accessed 28 Sept 2013) www.cenfri.org/documents/AML/AML_CFT%20and%20Financial%20Inclusion.pdf
[18] Isern, J., and L. De Koker (2009) *AML/CFT: Strengthening Financial Inclusion and Integrity*, Focus Note 56. (CGAP, Washington, DC) www.cgap.org/gm/document-1.9.37862/FN56.pdf (accessed 28 Sept 2013)
[19] For example, refer to a recent publication commissioned by the United Nations and the Norwegian Refugee Council on the perspective of aid organisations. Mackintosh, Kate & Patrick Duplat (2013) 'Study of the Impact of Donor Counter-Terrorism Measures on Principled Humanitarian Action,' UNOCHA/NRC https://docs.unocha.org/sites/dms/Documents/CT_Study_Full_Report.pdf

Tom Keatinge
September 2013

Written evidence submitted by the Henry Jackson Society [CT 09]

The Henry Jackson Society (HJS) is a London-based think-tank founded on the global promotion of the rule of law, liberal democracy and civil rights. HJS specialises in the study of international terrorism, counter-terrorism and radicalisation. This submission is a corporate view, based on original research and institutional expertise.

How effective is the Government in working with foreign Governments and Multi-lateral organisations to counter terrorist threats at home and abroad?

1. After 11 September 2001, close intelligence cooperation is a necessity. This cooperation must be discreet, as it touches on sensitive, sovereign areas like intelligence and justice; as well as focuses on operational issues, for example, preventing planned terrorist attacks. As such, the United Kingdom (U.K.) believes that cooperation is more effective in a bilateral arena rather than a multilateral one.[1]

2. The U.K. is not alone in privileging bilateral relations. The United States (U.S.) prefers to cooperate with individual European Union (E.U.) member states rather than with the institution as a whole. Where speed, trust and flexibility are needed, individual partnerships have proven the most reliable forum for preventing terrorism. The U.S., for example, has praised the U.K.'s legal and administrative ability to take action against terrorists and their supporters, including asset freezing as well as its intelligence sharing, terrorist cells arrests and terrorist financing and logistics interdiction.

3. For security reasons and to minimise the risk of leaks, the U.K. rarely uses multilateral organisations. The majority of counter-terrorism cases in the U.K. do not involve other countries in the E.U. When it does, the U.K. prefers to co-operate directly with the security services of that particular country. The U.K. has a good reputation for bilateral counter-terrorism work.

4. The Home Secretary Theresa May has suggested that the U.K. should leave Europol in 2015, despite the recommendations of her senior advisors. The U.K. is expected to withhold support for a revamped Europol, which includes a merger with the European Police College, amid complaints that the restructure could restrict the independence of British police forces.

5. The Association of Chief Police Officers called the move a 'massive step back for U.K. policing', and the British director of Europol, Rob Wainwright, said: 'It is undeniable that the demands of fighting international crime and terrorism require an ever-increasing level of co-operation between the member states.'[2] This will further damage the U.K.'s reputation within multilateral law enforcement organisations.

6. U.K. interaction with Europol is rare, and when Europol contacts the U.K. for specific information, it is often either incomplete or not provided. In comparison to other E.U. countries, such as Germany, the U.K. does not send many representatives to Europol. Also, unlike other E.U. countries, the U.K. utilises a liaison officer to Europol rather than a dedicated counter-terrorism official.

[1] Information in t this section is taken from interviews with senior Europol officials.
[2] 'Met's Madeleine McCann hunt "at risk" if UK opts out of Europol', *Independent*, 7 July 2013, available at http://www.independent.co.uk/news/uk/crime/mets-madeleine-mccann-hunt-at-risk-if-uk-opts-out-of-europol-8692657.html

7. Individual country's complex counter-terrorism structures can hamper internal and external dialogue. Harmonising such structures within partner countries could improve bilateral and international cooperation. A legal framework, for example, within which law-enforcement agencies could exchange information without encroaching countries' sovereign rights would function as a shared space to enhance co-operation and would allow for regional differences.

Are Terrorism Prevention & Investigation Measures effective as an investigation measure?

8. Terrorism Prevention & Investigation Measures (TPIMs) were introduced in order to control the threat posed by individuals who are thought to have engaged in Terrorism Related Activity (TRA) but cannot be prosecuted or deported.

9. According to the government's independent reviewer of terrorism legislation, the reference to 'investigation' in the legislation's title is 'a nod to the notion that subjects might, during the currency of a TPIM, engage in TRA which could be detected and then used as evidence in a criminal trial.'[3] A Senior Investigative Officer is assigned to each individual under a TPIM for this specific reason.

10. Part of the reason for this focus on prosecutions is that the Liberal Democrats' 2010 Manifesto stated that 'the best way to combat terrorism is to prosecute terrorists, not give away hard-won British freedoms'. To this end, they pledged to scrap Control Orders, the predecessor to TPIMs.[4]

11. However, to date, there have been no TPIM subjects successfully prosecuted for TRA. They have proven ineffective as an investigatory measure for a variety reasons.

12. Firstly, those being monitored are aware of the fact. If there was insufficient evidence for prosecution (hence the TPIM being issued), the chance of that evidence existing once the subject knows they are being monitored is minimal.[5] The restrictions that TPIMs place subjects under – e.g. a curfew, electronic tag and limitations on access to electronic items – makes them aware that committing an offence without the possibility of being caught is unlikely.

13. In this regard, the lack of prosecutions can be interpreted as a sign of success. It proves that TPIMs discourage TRA, with their effectiveness at prevention meaning there is little to investigate.

14. Secondly, unlike Control Orders, TPIMs have a fixed two year limit. They cannot be extended unless the subject commits new TRA. Any suspected terrorist is aware of the two year window constraining their activities.[6] Therefore, the likelihood of any suspect committing TRA that would lead to their prosecution is low. Logically, they are more likely to refrain from TRA for the two years it would take to remove their TPIM. Therefore in early 2014, many of those under TPIM when the legislation was introduced will have their restrictions removed.[7]

15. Therefore, the 'Investigation' aspect of TPIMs has essentially proven to be obsolete. This is unsurprising, as the very existence of TPIMs is a result of the fact that some national security threats are impossible to prosecute and public safety measures need to be taken.

[3] 'Terrorism Prevention and Investigation Measures in 2012: First Report of the Independent Reviewer on the Operation of the Terrorism Prevention and Investigation Measures Act 2011', Independent Reviewer of Terrorism Legislation (March 2013), p.70, available at http://www.official-documents.gov.uk/document/other/9780108512285/9780108512285.pdf
[4] 'Liberal Democrat Manifesto 2010', p. 94, available at http://network.libdems.org.uk/manifesto2010/libdem_manifesto_2010.pdf
[5] 'Terrorism Prevention and Investigation Measures in 2012', Independent Reviewer of Terrorism Legislation (March 2013), p.70
[6] Ibid.
[7] Ibid., p. 93

16. Control Orders were equally ineffective in leading to prosecutions. Of the nine people under Control Order arrested on suspicion of committing a terrorist offence, one (11%) was charged – and this for activities prior to being placed under a Control Order. Furthermore, this prosecution was unsuccessful. Therefore, there was a zero percent success rate in prosecuting Control Order subjects for terrorism offences.[8]

17. While TPIMs are of limited use as an investigatory measure, they more likely lead to convictions for a breach of the requirements they place on a suspected terrorist.

18. In June 2013, 'DD' became the first person under a TPIM to be convicted of this. He breached his TPIM three times, and was jailed for nine months.[9] Another, 'FF', has just been charged for the same offence.[10]

19. However, prosecutions are unlikely to be straightforward. For example, 'BM' was acquitted of breaching his TPIM in October 2102. Despite charges only usually being brought in such cases when a 'substantial number of breaches had been committed',[11] the jury accepted his explanation that he had simply forgotten about his requirement to attend a police station daily as part of his TPIM.[12]
20. During Control Orders' lifetime (2005 – 2011),[13] a total fourteen controlees were prosecuted for breach of their conditions, one on two separate occasions.[14]

21. Of this total of fifteen potential trials, six (40%) resulted in no evidence being offered by the prosecution, as the trial was not seen to be in the public interest. Only two (13%) led to convictions: 'MB' (jailed for twenty weeks) and 'BX' (jailed for fifteen months). Two (13%) were also acquitted; one controlee (7%) absconded; and another left the U.K. of his own volition (7%). As of March 2012, a further three (20%) were awaiting trial.[15]

22. There have been no convictions of Control Order or TPIM subjects based on TRA. A total of three have been convicted for breaches – yet substantially more cases have proven unsuccessful.

Has the Charity Commission reduced the ability of terrorists to obtain funding through charitable donations?

23. The Charity Commission has demonstrated limited abilities to tackle fundraising by U.K.-based charities for terrorist purposes, and, more broadly, to vet or disqualify unsuitable charitable trustees by virtue of their association with terrorism. Two cases exemplify these limitations: the failure to address Interpal's provision of financial support for the proscribed terrorist organisation Hamas;[16] and continued trusteeship of the Islamic Research Foundation International (IRF) by Indian cleric Dr. Zakir Abdul-Karim Naik despite a U.K. exclusion order against him on terrorism-related grounds.

[8] 'Terrorism Prevention and Investigation Measures in 2012', Independent Reviewer of Terrorism Legislation (2013), p. 70
[9] 'Suspected terrorist imprisoned over TPIM breaches', *ITV*, 21 June 2013, available at http://www.itv.com/news/central/update/2013-06-21/man-imprisoned-over-tpim-breaches/
[10] 'Somali man accused of terror order breach', *BBC News*, 21 September 2013, available at http://www.bbc.co.uk/news/uk-24188138
[11] 'Control Orders in 2011: Final Report of the Independent Reviewer on the Prevention of Terrorism Act 2005', Independent Reviewer of Terrorism Legislation (March 2012), p. 44, available at http://www.official-documents.gov.uk/document/other/9780108511417/9780108511417.pdf
[12] 'Ilford terror suspect "breached order keeping track of his movements", court is told', *Ilford Recorder*, 11 October 2012
[13] Details all cases up until the end of 2009 can be found in *Control Orders: Strengthening National Security*, The Centre for Social Cohesion (2010), available at http://henryjacksonsociety.org/wp-content/uploads/2013/01/CONTROL-ORDERS.pdf. In 2011, the Centre for Social Cohesion and all its employees merged with the Henry Jackson Society.
[14] 'Terrorism Prevention and Investigation Measures in 2012', Independent Reviewer of Terrorism Legislation (2013), p. 44
[15] 'Control Orders in 2011: Final Report of the Independent Reviewer on the Prevention of Terrorism Act 2005', Independent Reviewer of Terrorism Legislation (2012), p. 44
[16] The Terrorism Act 2000: Proscribed Organisations, House of Commons Library note, 7 January 2013, p. 8, available at: www.parliament.uk/briefing-papers/sn00815.pdf.

24. While Interpal (charity no. 1040094) has been investigated by the Charity Commission for funding Hamas on three occasions, insufficient evidence was found in each case.[17] The U.S. Treasury, however, designated Interpal as a terrorist organisation in 2003, stating that: '[it] has been a principal charity utilized to hide the flow of money to Hamas' and that it is 'a coordination point for other Hamas-affiliated charities'.[18] Furthermore, the U.K. Foreign and Commonwealth Office has stated that, 'Hamas's political wing is represented [in the U.K.] by charitable organisations which raise and remit funds for welfare purposes'.[19]

25. The perceived separation between Hamas's political and military wings has been denied by senior Hamas members,[20] who acknowledge that welfare programmes are designed to keep 'the flame of Jihad alight'.[21] Interpal was conceived as part of an international Hamas project to solicit funding;[22] and has consistently funded Hamas social welfare programmes via Hamas-controlled charities in Gaza and the West Bank.

26. The Charity Commission's failure to prove the allegations can be attributed to a lack of resources. Terrorist fundraising cases are handled by the London-based Compliance Investigations Unit (CIU), part of the Compliance Division.[23] In a 2010 interview, the head of the division acknowledged that it kept 'as small a unit as possible in London for high-risk cases' and that an allegation of links to terrorism does not guarantee an investigation.[24] In 2010-2011, the CIU handled sixteen terrorism-related investigations;[25] but the Interpal case suggests that it lacks the resources for complex terrorist financing investigations, including requirements for foreign travel, translation services or security measures.

27. The 1996 investigation into allegations that Interpal funded the families of Hamas suicide bombers, for example, concluded that the charity did not hold records containing family details of the intended beneficiaries. The investigation was limited, however, to Interpal's London office and failed to investigate how Interpal's recipient Palestinian charities identified their beneficiaries.[26] Similarly, the 2003 investigation into Interpal failed to interview an overseas ally who had obtained documents stating that Interpal was one of the four primary financial sources for Hamas.[27] A Charity Commission spokesperson subsequently told the BBC's Panorama that the 2003 investigation was 'not in-depth'.[28]

[17] Investigations were opened in 1996, 2003 and 2006; Interpal's predecessor, the Palestine Lebanon Relief Fund, was also investigated in 1996.
[18] U.S. Designates Five Charities Funding Hamas and Six Senior Hamas Leaders as Terrorist Entities, U.S. Department of the Treasury, 22 August 2003, available at: http://www.treasury.gov/press-center/press-releases/Pages/js672.aspx; see also 'Additional Background Information on Charities Designated Under Executive Order 13224' U.S. Department of the Treasury, available at: http://www.treasury.gov/resource-center/terrorist-illicit-finance/Pages/protecting-charities_execorder_13224-i.aspx#i.
[19] The Terrorism Act 2000: Proscribed Organisations, p. 26.
[20] Hamas founder Sheikh Ahmed Yassin, for example, told Reuters on 27 May 1998 that, 'We cannot separate the wing from the body. If we do so, the body will not be able to fly. Hamas is one body'.
[21] 'Memo prepared by Hamas Political Bureau in 2000 just before the eruption of 2nd Intifada', in Azzam Tamimi, *Hamas, Unwritten Chapters*, (London: Hurst & Co, 2007), pp. 254-255.
[22] 'Memo prepared by Hamas Political Bureau in 2000 just before the eruption of 2nd Intifada'
[23] The role of Compliance Division, Charity Commission, available at: https://apps.charitycommission.gov.uk/Our_regulatory_activity/Our_approach/compman.aspx
[24] 'Interview: Michelle Russell, head of the Charity Commission's compliance division', Third Sector, 2 March 2010, available at: http://www.thirdsector.co.uk/Governance/article/986668/Interview-Michelle-Russell-head-Charity-Commissions-compliance-division/.
[25] Counter-terrorism strategy, Charity Commission, available at: http://www.charitycommission.gov.uk/our_regulatory_activity/counter_terrorism_work/ctstrategy.aspx#sthash.gxfpq5ja.dpuf.
[26] Interview with John Ware, reporter of the BBC Panorama's 2006 investigation of Interpal, 'Faith, hate and charity'.
[27] Interview with John Ware; details of the seized material can be found at the Intelligence and Terrorism Information Center, available at: http://www.terrorism-info.org.il/en/index.aspx
[28] 'Faith, hate and charity' (transcript), BBC Panorama, 30 July 2006, available at: http://news.bbc.co.uk/1/hi/programmes/panorama/5234586.stm

28. There is also inadequate monitoring following an investigation. The Charity Commission, for example, did not ensure that Interpal had complied with the recommendations of its 2003 investigation: during the 2006-2009 investigation it became aware that Interpal had not sought clarification from its recipient charities regarding their procedures for identifying beneficiaries.[29] Interpal had said it would invite international NGOs to independently verify the distribution of its funds, when in fact these NGOs were members of the Union of Good (UoG), an umbrella organisation established by Interpal in 2001,[30] which was designated as a terrorist organisation by the U.S. Treasury in November 2008 for transferring money between international charities and Hamas.[31]

29. The Interpal case demonstrates that the CIU is not flexible enough to respond to charities' efforts to circumvent regulation. In 2009, the CIU legally directed Interpal trustees to end the charity's membership with the UoG because 'its members included designated entities';[32] and a 2012 case review concluded that Interpal had complied.[33] Since 2009, however, Interpal trustees have continued their involvement with both the UoG and senior Hamas leaders, as well as organised multiple 'Miles of Smiles' aid convoys providing cash and supplies to Hamas.[34] The UoG Arabic website, for example, listed Interpal as late as March 2012;[35] and Interpal employees have been photographed on numerous occasions sharing political platforms with Hamas leaders. [36]

30. The Charity Commission directive was limited to the UoG, rather than the individuals or organisations it represents or new manifestations of the organisation. As such, the Charity Commission fails to recognise the efforts of Interpal trustees to obfuscate their connections to UoG members and other designated organisations or individuals.

31. In a broader sense, the Charity Commission has failed to challenge trustees who support Islamism-inspired terrorism. Currently, there is no legal mechanism to prevent individuals convicted for terrorism-related offences or excluded from the U.K. on terrorism-related grounds from becoming a charitable trustee. Such omission runs counter to the government's 2011 commitment that it would no longer engage with or fund groups that fail to support British values or act as apologists for terrorist organisations.[37]

32. Dr. Zakir Naik, for example, was excluded from the U.K. in June 2010 on the grounds that some of his public statements 'justif[ied] terrorist violence and foster[ed] hatred' and may have

[29] 'Palestinians Relief and Development Fund (Interpal), Charity Commission Inquiry', 27 February 2009, pp. 5 & 24–25; see also 'Charities Back on Track: Themes and lessons learned from the Charity Commission's compliance work' (2008–09), Charity Commission, 2009, p. 16, available at: http://www.charitycommission.gov.uk/media/91114/track09.pdf
[30] Interpal trustee Dr. Essam Yusuf told the Charity Commission during the 2006–2009 investigation that he was the 'originator' of UoG. See Response to Interpal inquiry by Charity Commission, BBC Panorama, 2 March 2009, available at:http://news.bbc.co.uk/panorama/hi/front_page/newsid_7915000/7915916.stm
[31] 'Defense Minister Signs Order Banning Hamas-Affiliated Charitable Organizations,' Israeli Ministry of Foreign Affairs, 7 July 2008, available at www.mfa.gov.il/MFA/Government/Communiques/2008/Defense+Minister+signs+order+banning+Hamas-affiliated+charitable+organizations+7-Jul-2008.htm; See also Treasury Designates the Union of Good, US Department of the Treasury, 12 November 2008, available at: available at http://www.treasury.gov/press-center/press-releases/Pages/hp1267.aspx.
[32] Charities Back on Track (2008–09), p.16.
[33] Palestinians Relief and Development Fund (Interpal) - supplementary report, 1 June 2012
[34] 'Miles of Smiles 13' convoy arrives in Gaza', Ezzedeen Al-Qassam Brigade Information Office, 12 June 2012, available at: http://www.qassam.ps/news-5814-Miles_of_Smiles_13_convoy_arrives_in_Gaza.html
[35] An archived webpage (http://www.eetelaf.org/donation.html) dated 2 March 2012 is available at: http://web.archive.org/web/20120302150253/http://www.eetelaf.org/donation.html
[36] See, for example, 'Interpal visits Hamas again', *Harry's Place*, 2 August 2011, available at: http://hurryupharry.org/2011/08/02/interpal-visits-hamas-again/
[37] Prevent Strategy, HM Government, June 2011, pp. 1 & 8, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf

influenced those engaging in terrorist acts, including the 2006 and 2008 Mumbai attacks.[38] Dr. Naik continues to act as a trustee of the IRF (charity no. 1122086).[39] Moreover, the IRF was implicated in Dr. Naik's exclusion order: of the 11 statements listed, three came from a 2007 IRF conference;[40] and one from the IRF website.[41] Financial statements show that IRF expends over £1million annually to 'support' its international TV channel, Peace TV, which Dr. Naik hosts.[42] Dr. Naik has previously stated on Peace TV that suicide bombings can be justified in Islam.[43]

Does the Government have the capability to examine and combat the use of communications (including via the internet) in TRA?

33. The most pervasive aspect of internet communications, social media, has connected the internet with environments such as university campuses, providing extremists with greater opportunity to carry out TRA. This presents the Government and law enforcement agencies with a number of significant challenges.

34. The Government is hampered in its ability to challenge the use of social media for TRA by the volume of material generated. Police officers state that despite efforts to include some monitoring of social media, forces are still reliant on the reporting of potential offences by the public. Monitoring social media is only one facet of a wider role, preventing the acquirement of detailed understanding and coverage.[44] To put the scale of the task into perspective, in June 2012 Twitter estimated that 400 million tweets were sent every day.[45] In a five day period encompassing the Woolwich Barracks attack, 19,344 tweets were addressed to the Metropolitan Police Twitter account, with 20.6% reporting a possible crime.[46]

35. The global nature of social media means an individual in one country can share web pages hosted in a second with an audience in a third. The Counterterrorism Internet Referral Unit was able to remove material from the internet on 156 occasions in the 15 months from its founding in 2010,[47] but the ease with which this material can be replaced (YouTube estimate that 100 hours of video are uploaded every minute)[48] and the reluctance of other countries and international firms to remove material makes this an almost impossible task.

36. These difficulties facilitate the commission of a number of terrorism-related offences via social media, the most relevant of which are: Soliciting or incitement to murder; Fundraising for terrorist purposes; Proscribed organisation offences; Distribution or possession of a terrorist publication; Encouraging terrorism; Possession of a document containing information likely to be useful to a person committing or preparing an act of terrorism.[49]

[38] Naik v Secretary of State for the Home Department & Anor [2010] EWHC 2825 (Admin) (05 November 2010), available at www.bailii.org/ew/cases/EWHC/Admin/2010/2825.html
[39] On 19 May 2011, the Charity Commission advised HJS that 'despite Dr Naik's exclusion from the U.K. he remains legally able to act as a trustee due to provisions within the governing document of the Islamic Research Foundation International in respect of trustee meetings.'
[40] Peace: the Solution for Humanity, An international Islamic Conference & Exhibition, organised by the IRF, 23 November – 2 December, 2007, Mumbai, India; video available at www.youtube.com/watch?v=L83yIOztJ5g
[41] FAQ on Islam by Dr Zakir Naik, IRF website; archived version dates to 2003; available at web.archive.org/web/20080529022339/www.irf.net/irf/dtp/dawah_tech/mcqnm11.htm
[42] £1,396,883, according to the Report of the Trustees and Financial Statements for the year ended 31 January 2012 for Islamic Research Foundation International, available at: http://apps.charitycommission.gov.uk/Accounts/Ends86/0001122086_ac_20120131_e_c.pdf
[43] Q&A with Zakir Naik, Peace TV, undated, available at http://www.youtube.com/watch?v=UCUjdmUQ5E4&feature=player_embedded
[44] Interviews with serving Counter-Terrorism Unit and Prevent Officers
[45] 'Twitter in Numbers', *Telegraph*, 21 March 2013, available at http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html
[46] '@MetpoliceUK: How Twitter is Changing Modern Policing', *Demos*, June 2013
[47] HM Government, Prevent Strategy, p. 78
[48] 'Statistics', YouTube, available at http://www.youtube.com/yt/press/statistics.html
[49] See 'Challenging Extremists: Practical Frameworks for our Universities', Student Rights – The Campus Project of the Henry Jackson Society (2012) p. 62

37. For example, in the academic year 2011/12 an individual used Facebook to share material with students at the University of Westminster which included two video slideshows showing insurgent fighters posing with weapons and engaged in firefights.[50] One featured voiceover by the former Al-Qaeda cleric Anwar Al-Awlaki, and the other by Abdul Rahman Saleem, convicted of inciting racial hatred in 2007 and inciting others to kill coalition soldiers in Iraq and Afghanistan in 2008.[51] A third video shared was of Yassin Chouka, a Specially Designated Global Terrorist.[52]

38. The Abdul Rahman Saleem audio shared is extremely similar to the speech which formed the basis of his 2008 conviction, and it is likely that in sharing this material the same offence was committed. Yassin Chouka's designation as an Al-Qaeda-associated figure, and his alleged position in Jundallah Media,[53] would also suggest that the sharing of this video would constitute a dissemination of terrorist publications offence.

Henry Jackson Society
September 2013

[50] 'Challenging Extremists: Practical Frameworks for our Universities', Student Rights (2012), p. 20-22
[51] 'Islamist Terrorism: The British Connections', Henry Jackson Society (2011), p. 95-96
[52] The Designation of Yassin Chouka, also known as Yasin Chouka, also known as Abu Ibrahim, also known as Abu Ibraheem the German, also known as Abu Ibrahim al Almani, as a Specially Designated Global Terrorist pursuant to Section 1(b) of Executive Order 13224, as Amended, State Department notice, 2 February 2012, available at https://federalregister.gov/a/2012-2348; United Nations Security Council, Security Council Committee pursuant to resolutions 1267 (1999) and 1989 (2011) concerning Al-Qaida and associated individuals and entities, available at http://www.un.org/sc/committees/1267/
[53] Jundallah Media is the media arm of the Islamic Movement of Uzbekistan, an Al-Qaeda-linked organisation proscribed by the British government .

Written evidence submitted by the Financial Conduct Authority [CT 10]

1. This memorandum sets out the Financial Conduct Authority's (FCA's) role in supervising banks and money service businesses (MSBs) in relation to money laundering and terrorist financing. In particular, it sets out:
- The FCA's role and responsibilities, including our financial crime responsibilities;
- Our recent work in combatting financial crime; and
- How we work with other agencies.

FCA's role and responsibilities

2. The FCA was established on 1 April 2013. Our overall objective is to ensure that relevant markets work well. This is supported by three operational objectives, which are to:
- protect and enhance the integrity of the UK financial system;
- secure an appropriate degree of protection for consumers; and
- promote competition in the interests of consumers.

3. We are responsible for regulating the conduct of around 26,000 financial firms and for the prudential supervision of 23,000 that are not regulated by the Prudential Regulation Authority. We also regulate some important parts of UK market infrastructure and we are the UK's Listing Authority for securities issuers raising capital on UK markets. We promote innovation and healthy competition between financial services firms, and help them keep to the rules and maintain high conduct standards.

Financial crime responsibilities

4. In carrying out our work we have a duty under the Financial Services and Markets Act 2000(FSMA) to have regard to the importance of taking action intended to minimise the extent to which it is possible for firms to be used for financial crime. We are also the anti-money laundering (AML) and counter terrorist financing (CTF) supervisor of most financial services[1] firms subject to the Money Laundering Regulations 2007 (MLRs).

5. All FSMA-authorised firms must put in place systems and controls to enable them to identify, assess, monitor and manage money laundering risk, including the risk of terrorist financing. In addition, all firms who are subject to the MLRs (the exceptions being mortgage brokers, general insurers and general insurance brokers) must put in place systems and controls including effective and risk basked customer due diligence and ongoing monitoring procedures.

6. We are responsible for the supervision of banks' compliance with the MLRs and our rules. We are also responsible for overseeing firms compliance with any direction issued by the Treasury under schedule 7 of the Counter Terrorism Act 2008 in relation to risks of nuclear proliferation.

7. The FCA focuses on a firm's systems and controls to prevent money laundering. As a result, having effective systems, including checking the identity of customers at the opening of an account and monitoring ongoing transactions should assist the firm in protecting itself from being misused by those seeking to fund terrorism.

[1] This includes amongst others banks, building societies, stockbrokers, e-money institutions and safe custody services. From 1st April 2014 the FCA will also be responsible for supervising consumer credit firms subject to the MLRs.

8. HMRC is the AML supervisor for Money Service Businesses (MSBs) under the MLRs. The FCA is only responsible for AML supervision where MSBs are already authorised with the FCA for another activity e.g. a bank providing money transmission services.

9. Under the Payment Services Regulations 2009 we are responsible for overseeing the conduct of business and prudential requirements for firms offering payment services, which includes those MSBs who provide money transmission. We are responsible for ensuring they comply with the relevant legislation and regulation and consumers using their services are protected. However, this does not include responsibility for AML.

Recent financial crime work

AML report

10.As the Committee is aware, in response to your report *'Drugs: Breaking the Cycle*', we committed to publishing a report on the performance of our duties under the MLRs 2007. On 25 July, we published our first AML annual report which set out our AML obligations, how we meet those obligations and the trends and emerging risks in money laundering and terrorist financing that we are seeing in the firms we regulate.[2]

11.One of the issues we highlighted in our report that may affect FCA-regulated firms included the risk that the MSB sector may be used to launder money or finance terrorism. Our report stated that "the Money Service Business (MSB) sector as a whole is assessed by law enforcement as being at particularly high risk of abuse by those seeking to launder money or finance terrorism, and some MSBs have been seen to be complicit in these activities".

Systematic Anti-Money Laundering Programme

12.An important strand of our supervisory work continues to be our in-depth periodic probes in the UK's biggest banks – our Systematic Anti-Money Laundering Programme (SAMLP). This currently covers 14 major retail and investment banks operating in the UK. The SAMLP covers AML, counter-terrorist financing and financial sanctions.

Enforcement

13.An essential factor of our regulatory toolkit is enforcement action against the firms we regulate. Our enforcement action has focused on the issue of high risk customers/politically exposed persons (PEPs) over the past few years. This includes:

- Guaranty Trust Bank: £525,000 fine (August 2013) - failings in AML controls for high risk customers, including PEPs;
- EFG Private Bank: £4.2m fine (April 2013) – failings in AML controls for high risk customers, including PEPs;
- Turkish Bank (UK) Ltd: £294,000 fine (August 2012) – failings in AML controls over correspondent banking.
- Habib Bank AG Zurich: £525,000 fine and Money Laundering Reporting Officer fined £17,500 (May 2012) – failings in AML controls over high risk customers, including PEPs.
- Coutts & Co: £8.75m fine (March 2012) – failings in AML controls relating to high risk customers, including PEPs.

[2] http://www.fca.org.uk/static/documents/anti-money-laundering-report.pdf

Trade Finance thematic review

14.On 1 July we published our thematic review into trade finance in UK based banks.[3] Trade finance is internationally recognised as posing a high financial crime risk so the UK's position as a major financial centre could be severely impacted if banks engaging in trade finance do not have appropriate systems and controls to prevent financial crime.

15.The review into 17 banks found that they had generally developed effective controls to ensure they were not dealing with sanctioned individuals and entities, but most had failed to adequately consider money laundering and terrorist financing risk in trade finance.

Financial Crime Guide

16.We provide details of our expectations of how FCA-regulated firms should tackle financial crime risks in our publication *'Financial crime: a guide for firms'*.[4] This document is the main repository of information about financial crime (including money laundering and terrorist financing) and contains numerous examples of good and poor practice. It is a living document and is where we place the guidance material that, after consultation, flows from our thematic reviews such as the trade finance review mentioned above.

Working with others

17. An essential factor of the FCA's financial crime strategy is working in partnership with Government, law enforcement, other supervisors and the private sector.

Government

18.We are a member of the Money Laundering Advisory Committee, co-chaired by the Treasury and the Home Office, which brings together representatives from law enforcement, government, industry and regulators to advise the Government on its approach to preventing money laundering in the UK. This committee also reviews industry guidance before it is approved by the Treasury.

Law enforcement

19.Alongside other agencies such as HMRC and the Serious Fraud Office, the FCA works in partnership with the Economic Crime Command (ECC) of the National Crime Agency (NCA). We attend the ECC committees that determine its priorities and coordinate multi-agency action in response to economic crime threats. The FCA also has a seat on the ECC board.

20.The ECC currently focuses on fraud against the individual, public sector bodies or private sector organisations. It has identified money laundering as one of four enablers for these frauds. The ECC sees tackling money laundering as important for reducing serious organised and/or complex economic crime and protecting the UK's reputation and economy.

21.The FCA receives occasional reports on individual cases from law enforcement agencies about money laundering investigations where there are concerns that FCA-regulated firms may have facilitated money laundering, either knowingly or though ineffective AML procedures. The FCA works with law enforcement to encourage their

[3] http://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf

[4] Financial crime: a guide for firms, Part 1: A firm's guide to preventing financial crime (http://media.fshandbook.info/Handbook/FC1_20130401.pdf) and Financial crime: a guide for firms, Part 2: Financial crime thematic reviews (http://media.fshandbook.info/Handbook/FC2_20130401.pdf)

financial investigators to pass more intelligence to us about poor AML practice by firms, to help us focus our supervisory efforts.

Other supervisors

22.The FCA collaborates with other anti-money laundering supervisors in the UK and in other jurisdictions. The Anti-Money Laundering Supervisors forum was set up by the supervisory authorities specified in the MLRs to share views on current and emerging concerns and best practice. The FCA plays a key role in this forum, as well as chairing the public sector group within the forum.

23.In relation to MSBs in particular, we regularly share information with HMRC about the firms that both organisations oversee, and arrange joint visits where appropriate. This is where the FCA regulates the firm under the Payment Services Regulation 2009 and HMRC is the AML supervisor. In addition, we support HMRC's work on MSBs. The FCA sits on the board of Project Quaver, a multi-agency approach to deal with the risk of MSBs and are supporting the Serious Organised Crime Agency in providing information on specific areas of risk to the industry and then working with the industry to share best practice in mitigating that risk.

Private sector

24.We work with the Joint Money Laundering Steering Group, which produces guidance for the financial services industry on preventing money laundering and combating terrorist financing.

Financial Conduct Authority

September 2013

Written evidence submitted by David Anderson Q.C. [CT 11]

Role of the Independent Reviewer

1. I am a QC in independent practice, a Visiting Professor at King's College London and a Recorder of the Crown Court. I have no political affiliation. I succeeded Lord Carlile CBE QC as Independent Reviewer of Terrorism Legislation in 2011: my three-year term (which is renewable) ends in February 2014. The role has two features rarely seen in combination: complete independence from Government; and unrestricted access, based on a high degree of security clearance, to classified information and national security personnel.

2. The principal statutory responsibility of the Independent Reviewer is to report annually on the operation of certain specific Acts of Parliament concerned with terrorism.[1] Those Acts govern significant elements of the *Pursue* strand of the Government's counter-terrorism strategy CONTEST. The most recent editions of my annual reports, each of which is relevant to the Committee's inquiry, are:

   (a) *The Terrorism Acts in 2012*, July 2013 (nature of the threat; the counter-terrorism machine; definition of terrorism; proscription; terrorist property; terrorist investigations; arrest and detention; stop and search; port and border controls; terrorist offences);[2]

   (b) *Terrorism Prevention and Investigation Measures in 2012*, March 2013 (TPIMs); and[3]

   (c) *Second report into the operation of the Terrorist Asset Freezing &c Act 2010*, December 2012 (terrorist asset freezing).[4]

   Other reviews are conducted from time to time. The Reviewer's reports are submitted to the Home Secretary or the Treasury, and must be laid before Parliament on receipt. They are not annexed for reasons of space but are freely available, along with other material, on the Reviewer's website.[5]

3. The original purpose of annual review – instituted in 1984 – was to inform the annual debates that were then required if terrorism laws were to be renewed. Since the repeal of the Prevention of Terrorism Act 2005 and its replacement by the TPIM Act 2011, annual renewals of anti-terrorism laws have ceased. The Reviewer's central function however remains to inform the public and political debate on terrorism and civil liberties. That

[1] I have recommended that subject to resources, the operation of two further anti-terrorism laws (ATCSA 2001 and CTA 2008) should also be considered for independent review: *The Terrorism Acts in 2011*, June 2012, 12.1.

[2] https://terrorismlegislationreviewer.independent.gov.uk/the-terrorism-acts-in-2012/

[3] https://terrorismlegislationreviewer.independent.gov.uk/report-on-terrorism-prevention-and-investigation-measures-act-2011-in-2012/

[4] https://terrorismlegislationreviewer.independent.gov.uk/report-on-the-terrorist-asset-freezing-etc-act-2010-in-20112012/

[5] www.terrorism-legislation-reviewer.independent.gov.uk

function is discharged by his reports and by the evidence that he is invited to give to Parliamentary Committees. Reports and evidence often draw on classified materials. The Reviewer's evidence and reports have been cited in Parliamentary debates[6] and in judgments of the courts both in the UK and in Strasbourg.[7]

4. I also post on my website, publish articles, give interviews to the media and lecture to public and professional audiences, universities and schools on counter-terrorism powers and civil liberties. Like my predecessor I participate regularly in police training, particularly in relation to Schedule 7, and have the opportunity, in regular private meetings with Ministers, officials, senior police officers and others, to communicate any sensitive concerns in a less formal context.

5. I travel widely within the UK in order to observe and discuss the operation of the anti-terrorism laws both with those responsible for their content and enforcement (Ministers, MPs from all parties, officials, intelligence agencies, prosecutors, police and judges) and with others who come into contact with them (NGOs, lawyers, academics, journalists, port operators, religious and community groups and the subjects of TPIMs, immigration detention and port stops). In 2012 I travelled also to the US and to various institutions of the EU and Council of Europe. Later this year I plan to visit Israel. My Special Adviser, Professor Clive Walker, keeps me abreast of academic writings and comparative developments.

Scope of this evidence

6. This document can give no more than an overview of some of the issues which the Committee has indicated that it wishes to consider, while referring it to the relevant passages of my recent reports. Other issues lie outside the range of my statutory responsibilities. The operation of anti-terrorism law in Northern Ireland features in my reports; but I have assumed that Northern Ireland-related terrorism falls outside the scope of the Committee's inquiry. Within the limits of my expertise, I should be happy to contribute more detail in relation to any specific issues on which it is felt that my assistance could be useful.

[6] E.g. during the passage of the Justice and Security Act 2013, and in debates on the proscription of organisations.

[7] See *Gillan and Quinton v UK* (2010) 50 EHRR 45 (Terrorism Act stop and search) and, most recently, *R v SSHD ex p Beghal* [2013] EWHC 2573 Admin (Schedule 7).

Does the UK have sufficient capability to detect, investigate and disrupt terrorist threats?

The terrorist threat

7. The nature and extent of the terrorist threat to the UK and its citizens, as it stood at mid-2013, is fully summarised in chapter 2 of my July 2013 Terrorism Acts report. That account bears no official endorsement but is informed by my briefings from JTAC and MI5 as well as by my own reading and enquiries. Jonathan Evans, then Director General of MI5, was not exaggerating when he said in 2012 that "*Britain has experienced a credible terrorist attack about once a year since 9/11*." Though the ability of al-Qaida core to direct complex plots from the FATA has declined in recent years, foreign influences remain important and self-organised plots are not limited to the activities of so-called "*lone wolves*". Indeed the will and capacity to commit 7/7 style atrocities in the United Kingdom may well still exist, as demonstrated by the Birmingham rucksack bomb plot of 2011. Significant numbers of British citizens have lost their lives abroad this year to terrorism, notably in the Algerian gas plant and Nairobi shopping mall attacks. In Great Britain, 43 persons were charged with terrorism-related offences during 2012 – a figure precisely in line with the average since 2001.[8]

8. The threat needs to be kept in perspective, however. MI5's coverage of would-be Islamist terrorists has markedly improved since 2005; and since July 2011 the threat level set by JTAC, though still judged "substantial" (i.e. that an attack is a strong possibility), has been consistently lower than it was for three years after August 2006, when threat levels were introduced. There have been no recent al-Qaida related atrocities in Europe on the scale of the Madrid or London bombings of 2004-05. Thankfully and due in no small part to the activities of police and intelligence agencies, not a single person was killed by terrorists in Great Britain between summer 2005 and spring 2013.[9]

Counter-terrorism capability

9. The UK's capability (via *Pursue*) to detect, investigate and disrupt terrorist threats is grounded in the laws whose operation is the main subject of my reports . The organisational effort is summarised at chapter 3 of my July 2013 report. The increase in the UK's counter-terrorism capacity since 2005 has been substantial. Its principal components, as I record at 3.8-3.9 of my report, are counter-terrorism policing (for which Government funding was £573m in 2012/13) and a significant share of the £2.1 billion Security and Intelligence Agencies budget. The Counter-Terrorism and Special Cases Division of the Crown Prosecution Service has a strong record of prosecutions and an impressive concentration of expertise.

[8] I consider the charging figures to be more informative than the figures for "*terrorism-related arrests*", which may be criticised for subjectivity: see *The Terrorism Acts in 2012* (July 2013) at 8.3-8.8.

[9] The killings of Mohammed Saleem and Drummer Lee Rigby in April and May 2013 were both investigated as terrorism by the police. Suspects have been charged with murder in each case.

Is the capability sufficient?

10. The UK's capabilities seem to me broadly appropriate to the threat as it currently stands. In general, our anti-terrorism laws are formidably strong. The Terrorism Act 2000, which had considerable international influence after 9/11, was conceived at the end of a 30-year period which saw some 3500 killed in the Troubles as well as numerous hijackings, hostage-takings, suicide bombings and terrorist attacks worldwide. Yet it has been repeatedly supplemented since 9/11 – most notably by the introduction of various models of executive detention and restraint[10] and by the characterisation as "*precursor crimes*" of much previously lawful behaviour.[11]

11. It will always be possible (subject to the UK's international obligations and the tolerance of the courts) to provide for more crimes, more intrusive powers of search, longer periods of detention, more surveillance and more aggressive enforcement. But such measures can address only the symptoms and not the causes of terrorism. Worse, they may promote damage to everyday freedoms, the victimisation of affected communities and the diversion of scarce public funds into the vain pursuit of zero risk.[12] It has been heartening to observe, during my time in post, that the great majority of those entrusted with the formulation and enforcement of our anti-terrorism laws – including civil servants, security officials and police – well understand how laws that are over-extended or misapplied can become counter-productive. This does not remove the risk of abuse in individual cases, or diminish the need for careful independent scrutiny: but it does mean that enforcement takes place against what I have observed to be a positive institutional background.

12. Over the past few years, the anti-terrorism laws and their operation have been cautiously liberalised in areas ranging from stop and search and retention of biometric data to detention periods and control orders.[13] In successive reports I have found the liberalisation – but also the caution – to be justified. I have pointed to gaps in protection,[14] though it is often difficult to do so publicly. I have also made recommendations for further change. A few such recommendations (for example the possibility of bail for those arrested under the Terrorism Act 2000)[15] have been rejected, at least for now. Others have been partially

[10] Detention of undeportable foreign nationals in Belmarsh (Anti-Terrorism Crime and Security Act 2001), replaced in turn by control orders (Prevention of Terrorism Act 2005) and TPIMs (Terrorism Prevention and Investigation Measures Act 2011).

[11] Particularly in the Terrorism Act 2006: see my report *The Terrorism Acts in 2011*, June 2012,

[12] Such measures may also encourage the terrorists. As Jonathan Evans of MI5 said in 2010: "*In recent years we appear increasingly to have imported from the American media the assumption that terrorism is 100% preventable and that any incident that is not prevented is seen as a culpable government failure. This is a nonsensical way to consider terrorist risk and only plays into the hands of the terrorists themselves.*" Ayman al-Zawahiri, the current leader of al-Qaida, confirmed the point in a recent message marking the 12th anniversary of 9/11: "*We must bleed America economically by provoking it, so that it continues its massive expenditures on security*."

[13] See the overview in my report *The Terrorism Acts in 2012* (July 2013), 1.7-1.11. The first two developments were prompted by judgments of the European Court of Human Rights, as was the requirement that the gist of the national security case against them be provided to control order and now TPIM subjects.

[14] See, e.g., *The Terrorism Acts in 2011* (June 2012), 7.74 and 9.70.

[15] *The Terrorism Acts in 2011* (June 2012), 7.71-7.73.

adopted or are currently in train: in particular, the review and amendment of Schedule 7 port powers[16] and the revocation of outdated and potentially unlawful proscription orders.[17]

13. The replacement of control orders by TPIMs –a decision not prompted by the courts – has proved particularly controversial. TPIMs are significantly less invasive of personal liberty than were control orders. But the former practice of requiring controlled persons to be relocated away from their home cities could be effective in disrupting networks and preventing absconds, and was found by the courts to be proportionate in most though not all cases. I have said only that dropping relocation was a proper course for Parliament to take on civil liberties grounds.[18] More significantly still, TPIM notices – unlike control orders – are limited to two years, unless new terrorism-related activity takes place. The practical effect of this may prove to be the removal of all constraints, with effect from early 2014, on a number of TPIM subjects – men who are believed by the Home Secretary, with the approval of the courts, to be dangerous terrorists .[19] But persons who can neither be put on trial nor deported cannot in a civilised society be constrained indefinitely; additional money for covert investigative techniques has been provided to police and MI5, leading to an assessment of no substantial increase in overall risk; and even the two years now permitted is a very strong power by international or indeed by historic British standards. For these and other reasons, following my predecessor Lord Carlile, who suggested the change, I have described it as an acceptable compromise.[20]

The effectiveness of the Government in working with foreign Governments and multilateral organisations to counter terrorist threats at home and abroad

14. The closeness of the intelligence relationship with the United States is well-known. I am not best placed to evaluate its overall effectiveness, though after a fact-finding trip to Washington DC in 2012 I did give evidence in connection with the Justice and Security Bill on the extent to which intelligence-sharing was liable to be damaged by US fears that the control principle would not be fully respected in the UK.[21]

15. The counter-terrorism relationship with our EU partners was the subject of my written evidence in December 2012 to the House of Lords European Union Committee, following discussions in London, Brussels and The Hague.[22] I observed how influential the UK approach to counter-terrorism has been in Europe. My evidence was written before the

[16] *The Terrorism Acts in 2011* (June 2012), chapter 9; *The Terrorism Acts in 2012* (July 2013), chapter 10.

[17] *The Terrorism Acts in 2011* (June 2012), chapter 4; *The Terrorism Acts in 2012* (July 2013), chapter 5.

[18] *Control Orders in 2011* (March 2012), 6.13-6.14; *TPIMs in 2012* (March 2013), 11.30-11.32.

[19] Descriptions of each current TPIM subject, taken from open sources, are given in *TPIMs in 2012* (March 2013), chapter 4. Two of them are believed to have been involved in the 2006 airline liquid bomb plot, and have been under control orders or TPIMs since 2007 and 2008 respectively. A number of others are believed to have links with terrorism in East Africa.

[20] *TPIMs in 2012* (March 2013), 11.33-11.38.

[21] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/Justice_and_Security_oral_evidence_for_clickable_pdf.pdf, evidence of 16 October, QQ 72-82.

[22] http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/Protocol36OptOut/VolofevidenceP36asat110113.pdf, pp. 1-4. That evidence was summarised and supplemented in *The Terrorism Acts in 2012* (July 2013), 3.17-3.23.

Government released detailed plans for the proposed Protocol 36 opt-out. Assuming that the UK is able to opt back into the measures that it wishes to be part of, I have no basis at present for questioning the Government's view that co-operation in tackling terrorism will not be unduly affected, though I intend to keep this under review.

Whether the UK supports allies in building capacity to investigate and prosecute terrorists based overseas

16. Capacity-building is important not only to strengthen the ability of other countries to deal with terrorism, but to protect the UK's intelligence agencies against accusations that by co-operating with other countries, they have been complicit in torture or other illegal acts.

17. I have been asked to speak to visiting delegations from a number of other countries about counter-terrorism law and practice in the UK, and the importance of independent review. I do not though have an overall picture of the effectiveness of the Government's capacity-building efforts.

How effective TPIMs are as an investigatory measure

18. I reported earlier this year that TPIMs can be effective in preventing terrorism-related activity, but that like their predecessors, control orders, they have not been effective as investigatory measures.[23] It is indeed difficult to see how (despite their name) TPIMs could succeed on both fronts. If a TPIM prevents terrorism-related activity, it must follow that there is no terrorism-related activity to investigate.

19. Controlled persons and TPIM subjects have been prosecuted (with mixed success) for breach of the restrictions placed upon them.[24] But such breaches do not generally amount to engagement in terrorism-related activity. These prosecutions serve to enforce the obligations in a TPIM, but cannot in themselves serve as a justification for the TPIM.

The possible implications of moving responsibility for counter-terrorism from the MPS to the NCA

20. I visit both the MPS and the regional police counter-terrorism units, each of which is run by the force in whose area it sits. All are part of the police Counter-Terrorism Network. The Network, which works in full and active partnership with counter-terrorism policing structures in Scotland and Northern Ireland, is generally accepted to be an effective way of moving assets around the country in support of the highest priority operations, as directed by the Senior National Co-ordinator, an officer of the MPS.

21. Given the existence of a functioning system and the importance of what it does, it was wise in my view to postpone a decision on counter-terrorism and the NCA until the NCA is fully operational. I express no view on the underlying issue, other than to emphasise, on the basis of my own observation:

[23] *TPIMs in 2012* (March 2013), 11.3-11.10. No former controlled person was ever successfully prosecuted for a terrorist offence: *Control Orders in 2011*, March 2012, 3.19-3.21, 3.51.

[24] *TPIMs in 2012* (March 2013), chapter 10.

(a) the need for efficient allocation of counter-terrorism resources, geographically and in terms of the potential for officers trained in counter-terrorism to be deployed where necessary to other policing activities; and

(b) the importance of police officers involved in public-facing counter-terrorism work (whether a house raid or a port stop) understanding the implications of their actions for the communities most affected.

David Anderson Q.C.

Independent Reviewer of Terrorism Legislation

September 2013

Supplementary written evidence submitted by David Anderson Q.C. [CT 11a]

RECOMMENDATIONS OF THE INDEPENDENT REVIEWER ON SCHEDULE 7 TO THE TERRORISM ACT 2000

INTRODUCTION

1. Giving evidence to the Committee on 12 November 2013, I was asked (Q80) to spell out what changes to the port powers contained in Schedule 7 to the Terrorism Act 2000, other than the welcome amendments which have already been proposed by the Government in the Anti-Social Behaviour Crime and Policing Bill 2013, I considered desirable.

2. During the Report stage debate in the House of Commons on 15 October 2013, Rt Hon Damian Green MP had already indicated that he expected the Independent Reviewer to make recommendations, and that the Government would wish to examine them carefully.[1] At second reading in the House of Lords two weeks later, Lord Avebury, citing the Deputy Prime Minister, expressed the hope that my recommendations would be available "*while it may still be of assistance to your Lordships in the passage of this Bill*".[2]

3. My observations on the operation of Schedule 7, based on site visits (to 12 airports and seaports in England, Scotland, Wales and Northern Ireland, St Pancras International Rail Terminal, Calais, Coquelles, the National Ports Analysis Centre and the National Border Targeting Centre) and discussions (with police, MI5, civil servants, affected communities and individuals and NGOs), are recorded in my three annual reports on the operation of Schedule 7.[3] In each of those reports I noted the considerable utility of the Schedule 7 power in the fight against terrorism, while indicating certain areas where it seemed to me that amendment should at least be considered.[4] Some but not all of those issues were addressed in the public consultation and in the Bill. Three which regrettably were not – the thresholds for exercise of the Schedule 7 powers, the treatment of electronic data and the use made of answers given under compulsion – are considered in this note.

4. A full set of recommendations would ideally have awaited the final outcome of the numerous legal cases referred to at paragraph 7 below – in particular the imminent judgment in the judicial review proceedings arising out of the detention of David Miranda at Heathrow Airport in August 2013. I am conscious also that as Independent Reviewer, my primary function is to inform (rather than participate in) the political and public debate on

[1] Hansard 15 Oct 2013 HC col 634.

[2] Hansard 29 Oct 2013 HL col 1524.

[3] D. Anderson, *The Terrorism Acts in 2012*, July 2013, chapter 10; *The Terrorism Acts in 2011*, June 2012, chapter 9; *Report on the operation of the Terrorism Acts in 2010*, July 2011, chapter 9: all freely available on my website www.terrorism-legislation-reviewer.independent.gov.uk.

[4] See, most recently, my report of July 2013 at 10.48-10.80.

the scope of anti-terrorism law. It seems likely however that amendment to Schedule 7 will reach Committee stage in the House of Lords within the next two weeks. In the circumstances, and bearing in mind the comments cited at paragraphs 1 and 2 above, I take this opportunity to expand upon the answer to Q80 that I gave orally on 12 November.

5. My recommendations are given at paragraphs 19, 30, 36, 39, 40, 41 and 43 below, and set out together on the last page of this note.

6. I announced in August my intention of publishing a report into the detention of Mr Miranda. It soon became clear that much of the relevant ground would be authoritatively covered in his judicial review proceedings, which have been expeditiously handled on all sides and in which argument was heard on 6 and 7 November. Once judgment is handed down, I propose to decide what more I can usefully add, including by way of any additional recommendations relating to Schedule 7.

DEVELOPMENTS SINCE JULY 2013

7. The four months since my last report have been the most eventful in the long history of Schedule 7.[5] In addition to the progress of the Bill through Parliament, they have seen:

   (a) the publication in July of the Government's response to the public consultation on Schedule 7 which I had recommended in my 2011 report and which was conducted in late 2012, attracting 395 responses;[6]

   (b) the detention in August of David Miranda under Schedule 7 at Heathrow, giving rise to a storm of media controversy and a claim for judicial review, not yet decided, which raised a number of issues including the scope of the Schedule 7 power and its use in relation to what is said by Mr Miranda to be journalistic material;

   (c) the rejection in August by the Divisional Court of a claim by a French national, examined at Heathrow, that the application of Schedule 7 contravened Articles 5, 6 and 8 of the ECHR and EU free movement rules;[7]

   (d) a Liberal Democrat conference motion in October, calling for further safeguards;[8]

   (e) the publication in October of an "*illustrative*" draft revised Code of Practice for examining officers;[9]

[5] As was noted in *Beghal v DPP*, Schedule 7 was introduced in 2000 but derived from a temporary power introduced in 1974, at the height of the Troubles: [2013] EWHC 2573 (Admin), [36].

[6] *Review of the Operation of Schedule 7: A Public Consultation*, Home Office, July 2013.

[7] *Beghal v DPP* [2013] EWHC 2573 (Admin) (Gross LJ, Swift and Foskett JJ). The court is understood to have certified points for a possible appeal to the Supreme Court.

[8] Quoted in *Schedule 7 of the Terrorism Act 2000*, House of Commons Library Standard Note SN/HA/6742 (Joanna Dawson), 11 October 2013.

[9] *Draft Code of Practice for examining officers under Schedule 7 to the Terrorism Act 2000*, Home Office October 2013.

(f) a report in October by the Joint Committee of Human Rights, making a number of recommendations for the further reform of Schedule 7;[10]

(g) a Supreme Court *dictum* in October, in a judgment written by its President and the recently-retired Lord Chief Justice and concurred in by five other Justices, expressing concern about the breadth of the powers given to ports officers by Schedule 7;[11]

(h) the grant in November of a declaration that the refusal of police officers to await the arrival of a solicitor requested by a person detained under Schedule 7 before putting further questions to him was unlawful;[12] and

(i) a ministerial response of 11 November 2013 to the JCHR's report on the Bill, pp.11-17 of which respond to the Committee's recommendations on Schedule 7.

8. The blizzard of litigation has not yet abated. As well as possible appeals in *Beghal* and *Elosta*, judgment is currently awaited both from the Divisional Court in *Miranda* and from the European Court of Human Rights in an application (*Malik*), sponsored by Liberty, which claims that the exercise of Schedule 7 powers violated Articles 5(1) and 8 of the ECHR.[13] Other cases have also been brought.[14] It is plain that the passage of the Bill cannot await the final word from the courts in all these matters.

THRESHOLDS FOR THE USE OF SCHEDULE 7 POWERS

Legal background

9. The no-suspicion basis on which the Schedule 7 powers can be used was recently highlighted by the Supreme Court in *R v Gul* as a potential matter for concern.[15] It was also one of the

[10] Joint Committee on Human Rights, *Legislative Scrutiny: Anti-Social Behaviour, Crime and Policing Bill*, Fourth Report of Session 2013-2014, HL Paper 56 HC 713, 11 October 2013, chapter 4.

[11] *R v Gul* [2013] UKSC 64, (Lords Neuberger, Lady Hale, Lord Hope, Lord Mance, Lord Judge, Lord Kerr, Lord Reed), [63]-[64]. Having remarked on the broad prosecutorial discretion where terrorist offences are concerned, the Supreme Court continued: "*While the need to bestow wide, even intrusive powers on the police and other officers in connection with terrorism is understandable, the fact that the powers are so unrestricted and the definition of 'terrorism' is so wide means that such powers are probably of even more concern than the prosecutorial powers to which the Acts give rise. Thus, under Schedule 7 to the 2000 Act, the power to stop, question and detain in port and at borders is left to the examining officer. The power is not subject to any controls. Indeed, the officer is not even required to have grounds for suspecting that the person concerned falls within section 40(1) of the 2000 Act (ie that he has 'committed an offence' or he 'is or has been concerned in the commission, preparation or instigation of acts of terrorism'), or even that any offence has been or may be committed, before commencing an examination to see whether the person falls within that subsection. On this appeal we are not, of course, directly concerned with that issue in this case. But detention of the kind provided for in the Schedule represents the possibility of serious invasions of personal liberty.*"

[12] *R (Elosta) v MPC* [2013] EWHC 3397 (Admin): Bean J. I had expressed my own concerns on this point in *The Terrorism Acts in 2011* (June 2012), 9.66.

[13] Application no. 32968/11 *Malik v United Kingdom*, declared admissible on 28 May 2013.

[14] e.g. *Fiaz v GMP and SSHD*, a damages claim alleging discrimination in the application of Schedule 7.

[15] *R v Gul* [2013] UKSC 64, [63]-[64].

factors which led the European Court of Human Rights to hold that the no-suspicion stop and search power under sections 44-45 of the Terrorism Act 2000 was "*neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse*".[16]

10. As against that, both the Strasbourg institutions and the English courts have shown themselves willing, on occasion, to extend a wider margin of tolerance to the exercise of policing powers at the frontier than elsewhere.[17]

11. The purpose of this note is not to offer legal advice, or to predict the outcome of pending or future litigation before the senior courts of the UK or the Council of Europe. It seems fair to assume however that in any assessment of the Schedule 7 powers against the principles of the ECHR, the extent of the discretion given to examining officers will form an important part of the assessment of whether those powers are sufficiently circumscribed, necessary and proportionate.

The Schedule 7 powers

12. The central powers contained in Schedule 7 are the power to question (or examine) a person believed to be travelling through a port,[18] and an accompanying power of search.[19] For the purposes of exercising the power to question, an officer can stop a person or vehicle or detain a person.[20] Under the proposals in the Bill, a person will have to be detained if it is wished to question him for longer than an hour. Detention triggers the provisions of Part I of Schedule 8, which include both rights (to have a named person informed and to consult a solicitor)[21] and obligations (to submit in specified circumstances to the taking of fingerprints or samples).[22]

13. I drew attention in my annual reports to the practice of downloading the contents of mobile phones and other electronic devices (and of requiring the passwords to be handed over on request), and questioned its legal basis. The Government asserted that the necessary legal powers already existed under Schedule 7, but has also proposed a new paragraph 11A for Schedule 7, entitled "*Power to make and retain copies*", which would permit copies to be made of "*anything*" obtained pursuant to paragraphs 5, 8 or 9, and would permit those copies to be retained for so long as is necessary for the purpose of determining whether a person falls within section 40(1)(b), or while the examining officer believes that it may be needed for use as evidence in criminal proceedings or in connection with a deportation decision.[23]

16 *Gillan and Quinton v UK* (2010) EHRR 45.

17 *McVeigh v UK* (1981) 5 EHRR 71 (ECommHR); *Beghal v DPP* [2013] EWHC 2573 (Admin), [89]-[91]; Application 26291/06 *Gahramanov v Azerbaijan,* ECtHR 15 October 2013, [39]-[40].

18 Schedule 7, paras 2-3, 5.

19 Schedule 7, paras 7-9. The Bill proposes to prohibit intimate searches.

20 Schedule 7, para 6.

21 Schedule 8, paras 6-9.

22 Schedule 8, paras 10-14. The Bill proposes to remove the power to take an intimate sample.

23 On this issue see D. Anderson, *The Terrorism Acts in 2012*, July 2013, 10.65-10.73.

The current thresholds

14. The ***power to question*** (or examine) a person may only be exercised "*for the purpose of determining whether he appears to be a person falling within section 40(1)(b)*": in other words, a person who "*is or has been concerned in the commission, preparation or instigation of acts of terrorism*".[24] The courts may declare an examination to have been unlawful if this condition was not satisfied.[25] The examining officer may however exercise this power "*whether or not he has grounds for suspecting that a person falls within section 40(1)(b).*"

15. The ***powers to stop and detain*** may be used for the purposes of exercising the power to question, and are likewise subject to no requirement of suspicion.[26] A person who is examined can be compelled to provide any information in his possession, and to give the examining officer identity or other documents, again without any requirement of suspicion.

16. The ***power of search*** may also be used only for the purpose of determining whether a person who is questioned appears to be or to have been concerned in the commission, preparation or investigation of acts of terrorism.[27] No suspicion is required for the exercise of this power, save in the case of a strip search for which (under a proposal in the Bill) reasonable suspicion would be required, together with the authority of a supervising officer.

17. No requirement of suspicion attaches to the ***power to copy or download*** that would be created (or confirmed) by the proposed new paragraph 11A.

18. The ***power to take DNA samples*** may be used only if an officer of at least the rank of superintendent is satisfied that it is "*necessary in order to assist in determining whether [a person] falls within section 40(1)(b)*".[28] The ***power to take fingerprints*** may additionally be used if that officer has reasonable grounds for suspecting that a person is not who he claims to be.[29]

Powers to stop, question and search

19. ***I recommend that no change be made to the existing threshold for the exercise of the powers to stop, question and search, save for the amendment proposed in the Bill where strip search is concerned.*** My reasons for taking this position, which were based in part on confidential briefings and evidence from MI5, are set out in my 2013 report and remain valid.[30] A recent briefing on rules-based targeting at the National Border Targeting Centre has strongly confirmed me in this opinion.[31]

[24] Schedule 7, para 2(1); section 40(1)(b).
[25] As in *CC v MPS and SSHD* [2011] EWHC 3316 (Admin), [34].
[26] Schedule 7, para 6(1).
[27] Schedule 7, para 8.
[28] Schedule 8, para 10(6)(b).
[29] Schedule 8, para 6A(b).
[30] D. Anderson, *The Terrorism Acts in 2012*, 10.50-10.62. The reasons given at 10.58 include the need to preserve a deterrent against the use by terrorists of "*clean skins*", the need not to alert a traveller to the fact

20. The JCHR is largely of the same mind. It took the position, in its report of October, that "*the Government has clearly made out a case for a without suspicion power to stop, question and search travellers at ports and airports, given the current nature of the threat from terrorism, the significance of international travel in the overall threat picture, and the evidence seen by the Independent Reviewer demonstrating the utility of no-suspicion stops at ports in protecting national security*".[32]

21. This does not mean, of course, that the powers to stop, question or search may be used randomly or capriciously. The draft Code of Practice sets out a number of factors of the sort which examining officers need to have in mind when deciding whether to use their powers, before emphasising that:

> "*Schedule 7 powers are to be used solely for the purpose of allowing for the determination of whether the person examined appears to be, or to have been, concerned in the commission, preparation or instigation of acts of terrorism. The powers must not be used to stop and question persons for any other purpose.*"[33]

The courts will no doubt continue, if necessary, to declare an examination unlawful on the basis that it was not used for the statutory purpose.[34]

Power to detain

22. Despite currently being the subject of no higher threshold than the power to question, the power to detain is in general sparingly and responsibly used. Of the 61,145 persons examined under Schedule 7 in 2012/13, only 670 (1.1%) were detained. The majority of those, 547, had biometrics (fingerprints and/or DNA) taken, under the Schedule 8 power that is triggered by detention.[35]

that he is under surveillance and the need to question the unknown companion of a known terrorist. I also gave (at 10.59) examples of positive results which have been derived from untargeted no-suspicion stops.

[31] Rules based targeting involves the "washing" of carrier data against intelligence-led indicators (or rules), so as to flag those passengers most closely matching the chosen rules. A rule might, for example, be used in the counter-terrorism context to identify travellers with a profile similar to those of known terrorists travelling on routes of concern. Such targeting will not be enough to engender suspicion of each individual who is targeted: but it provides an entirely rational and potentially very useful way of identifying persons whom it may be appropriate to question, and if necessary to search, in order to determine whether they are concerned in the commission, preparation or instigation of acts of terrorism. See further John Vine QPM, "*Exporting the border? An inspection of e-borders October 2012-March 2013*".

[32] JCHR report, fn 10 above, para 110. The JCHR did however recommend a reasonable suspicion requirement before information on personal electronic devices could be accessed or searched: para 122.

[33] Home Office, *Draft Code of Practice for examining officers under Schedule 7 to the Terrorism Act 2000*, October 2013, para 19. The passage cited should however be moved above the sub-heading "*Examination period*", since it belongs under the previous sub-heading "*Exercise of Examination Powers and Selection Criteria*".

[34] As in the case of *CC v MPS and SSHD* [2011] EWHC 3316 (Admin).

[35] D. Anderson, *The Terrorism Acts in 2012*, June 2013, 10.7. For context, it may be recalled that some 245 million passengers travel through UK airports, seaports and international rail terminals in 2010/11: *ibid.*, 10.8(b).

23. The fact that a discretion may in general be responsibly used is however no safeguard against abuse, and no reason not to restrict its use to cases where it is strictly necessary. There may indeed be pressure to detain greater numbers once the Bill has become law, as detention will then be the only lawful way to question a person for longer than an hour. In 2012/13, 2,277 (3.7%) of those questioned were examined for over an hour.

24. The JCHR recommended that the power to detain should be exercised only if the examining officer reasonably suspects that the person is or has been involved in terrorism.[36]

25. I agree with the JCHR that an additional threshold or thresholds should have to be crossed before a person is detained under Schedule 7. Detention is a significant step, as may be seen from the fact that it carries with it the automatic right to legal advice as well as the potential obligation to give fingerprints and DNA samples. To be kept for up to six hours, particularly at the start of an outbound journey, can also be highly disruptive to international travel. It is hard to think of any other circumstances in which such a strong power may be exercised on a no-suspicion basis.

26. Three possible thresholds occur to me. In ascending order of significance, they are:

    (a) The examining officer considering (or a senior officer being satisfied) that detention is ***necessary in order to assist in determining*** whether a person appears to be a person falling within section 40(1)(b) [i.e. a person who is or has been concerned in the commission, preparation or instigation of acts of terrorism;]

    (b) The examining officer considering (or a senior officer being satisfied) that there are ***grounds for suspecting*** that the person appears to be a person falling within section 40(1)(b); or

    (c) The examining officer considering (or a senior officer being satisfied) that there are ***reasonable grounds for suspecting*** that the person appears to be a person falling within section 40(1)(b).

27. As to those options:

    (a) The first ("*necessary in order to assist in determining*") is little more than a statement of the obligation that rests upon any officer whose decision is liable to infringe the Article 8 (or Article 5) rights of another person. It is based on the existing threshold for the taking of fingerprints or a DNA sample,[37] which the Government does not propose to amend, and resembles the "*necessity*" threshold that the Bill proposes to introduce for

[36] JCHR report, fn 10 above, paras 112-114.

[37] Schedule 8 to the Terrorism Act 2000, para 10(6)(b).

authorisation by the review officer of *continued* detention after a so far unspecified period.[38]

(b) The second ("*grounds for suspecting*") would echo the subjective belief standards already present in paragraphs 2(2)(b) and 2(4) of Schedule 7. It would require the officer to have formed a suspicion, whether on the basis of information supplied by others, behavioural assessment or even just intuition. It would however ensure that (in the words of Lord Bingham, in the context of a stop and search power) a ports officer is not deterred from detaining *"a person whom he does suspect as a potential terrorist by the fear that he could not show reasonable grounds for his suspicion*".[39]

(c) The third ("*reasonable grounds for suspecting*") is the default threshold for most stop and search powers, and was the solution favoured by the JCHR in relation to the detention power. It is related to (though not identical to) the proposal in the Bill that strip searches should be conducted only where the examining officer has "*reasonable grounds to suspect that the person is concealing something which may be evidence that the person falls within section 40(1)(b)*".[40]

28. My exposure at a variety of ports to the operational constraints under which ports officers operate inclines me, on balance, towards rejecting the reasonable suspicion standard as a condition for detention.[41] In particular:

a. Terrorists pose risks on a different scale to most other criminals: they have shown themselves capable of causing death and destruction on a massive scale.

b. Active terrorists are not numerous, and not easily identified as such. Factors such as location, demeanour or evasive behaviour in the street may well give rise to a reasonable suspicion that a person is carrying stolen or prohibited articles.[42] In the neutral port environment, an experienced officer's suspicion of involvement in something as specific as the commission, preparation or instigation of acts of terrorism may however be harder to substantiate objectively in the absence of

[38] Schedule 8 to the Bill, para 7(3). The necessity is there linked to "*exercising a power under paragraph 2 or 3 of that Schedule*": I prefer the more direct formulation suggested here.

[39] *Gillan and Quinton* [2006] UKHL 12, para 35. It appears that a requirement of subjective suspicion in section 44 might have gone part of the way at least to satisfying the European Court of Human Rights which stated of section 44 in the same case, *Gillan and Quinton v UK* [2010] EHRR 45: "*Not only is it unnecessary for [the officer] to demonstrate the existence of any reasonable suspicion; he is not required even subjectively to suspect anything about the person stopped and searched*".

[40] Schedule 8 to the Bill, para 3(3) at 5(b).

[41] I am conscious that the courts were historically "*loath to subject to any searching analysis the basis of police claims that they had reasonable suspicion*": D. Feldman, *Civil Liberties and Human Rights in England and Wales*, 2nd edn. 2002, p. 334. But it would be unsatisfactory to rely on the courts adopting an over-permissive interpretation of the reasonable suspicion standard. As the same author acknowledges, ECtHR case law, given domestic effect by the Human Rights Act 1998, "*makes it clear that the reasonableness of a constable's suspicion must be carefully assessed*".

[42] Under the reasonable suspicion power in section 1 of the Police and Criminal Evidence Act 1984.

specific intelligence, if only because such involvement is relatively speaking so unusual.

c. The opportunity to test the validity of an officer's subjective suspicion in the hour allotted for examination may in practice be very limited, particularly when suspicion attaches to a large number of persons travelling together, and when time is lost by language difficulties or the use of false identities.

d. Detention sometimes has to be imposed at the outset of the examination, because the person refuses to cooperate. Such behaviour from a person confronted with the exercise of counter-terrorism powers might awaken suspicion: but it could be hard to characterise it as reasonable suspicion of involvement in terrorism. Effectively to require in such cases that reasonable suspicion be shown immediately after the stop would also be contrary to my recommendation and that of the JCHR.

29. These reasons lead me to the view that the operational needs of the police can best be reconciled with the necessary safeguards on detention by selecting the first and second of the options set out above. For consistency, the same test should be applied by the reviewing officer at the periodic review provided for by the Bill.

30. **I therefore recommend that:**

(a) Detention be permitted only when a senior officer is satisfied that there are grounds for suspecting that the person appears to be a person falling within section 40(1)(b) and that detention is necessary in order to assist in determining whether he is such a person.

(b) On periodic review, a detention may be extended only when a senior officer remains satisfied that there continue to be grounds for suspecting that the person appears to be a person falling within section 40(1)(b), and that detention continues to be necessary in order to assist in determining whether he is such a person.[43]

Copying and retention of electronic data

31. As I have recorded in successive reports, data taken from mobile phones, laptops and pen drives at ports has been instrumental in convicting terrorists and has also been extremely useful in piecing together terrorist networks.[44]

32. Such data are however treated in just the same way as any other thing that may be the subject of a search under Schedule 7. There is no legal threshold either for the search or for the downloading (or copying) of data from an electronic device, other than the basic

[43] Replacing the test in Schedule 8 to the Bill, para 7(3) at (3).

[44] See most recently, D. Anderson, *The Terrorism Acts in 2012*, July 2013, 10.59-10.60 and 10.65-10.80.

requirements that a search must be for the purposes of determining whether a person falls within section 40(1)(b),[45] and that the examination of goods must be for the purpose of determining whether they have been used in the commission, preparation or instigation of acts of terrorism.

33. Measured against the privacy that is liable to attach to the contents of (for example) a mobile phone, these powers are strong ones indeed. Neither the current law nor the proposed new paragraph 11A places any limitations on the categories of data (address book, call log, texts, emails, photographs) that can be copied, or any threshold that must be satisfied before this takes place. This is despite the fact that, outside the port, a warrant would be required for such inspections. Furthermore, the Code of Practice asserts that the information which an officer may expect a person to produce for examination or inspection includes passwords to electronic devices. This contrasts, as the JCHR pointed out, with the regime under RIPA section 49 for requiring the disclosure of the key to electronic data that has come into the possession of any person by means of the exercise of a statutory power.

34. It is perhaps possible to equate the initial search and examination of an electronic device[46] to the powers that police, customs and airport security have to rummage through hand luggage – a search power which neither the JCHR nor I has recommended should be subject to any new threshold. While the search of an electronic device undoubtedly has the capacity to impact upon private life, it does not do so to a markedly greater extent than other types of search, and may help shorten the examination of a person whose device confirms the innocent story he tells in interview. Notwithstanding the absence of any procedure equivalent to RIPA section 49 – an uncomfortable discrepancy – it might even be considered acceptable to require the production of a password for this purpose, though I can well understand that this is an issue that the Government or indeed Parliament may wish to consider further.

35. It is otherwise, however, where the wholesale copying of personal data is concerned. Of the possible thresholds set out at paragraph 26 and discussed at paragraph 27, above, I consider that the second is once again the most appropriate. The first is not required, because the purposes for which copies may be retained are already set out in the proposed paragraph 11A(3):[47] but see further paragraph 37(c), below.

36. **I therefore recommend that the power under the proposed paragraph 11A to make and retain copies of things detained pursuant to paragraphs 5, 8 and 9, should apply to personal electronic devices and to the data stored on them only if a senior officer is satisfied that there are grounds for suspecting that the person appears to be a person falling within section 40(1)(b).**

[45] Schedule 7, para 8(1).

[46] Schedule 7 paras 8, 9.

[47] This would allow a copy to be retained for as long as is necessary for the purpose of determining whether a person falls within section 40(1)(b), or while the examining officer believes that it may be needed for use as evidence in criminal proceedings or in connection with a decision by the Secretary of State whether to make a deportation order under the Immigration Act 1971.

FURTHER SAFEGUARDS

37. The Schedule 7 regime appears anomalous in relation to the absence of other safeguards that appear in comparable legislative regimes. Thus:

    (a) Property may be detained for seven days, even in the absence of any belief that it may be needed for use as evidence in criminal proceedings or in connection with a deportation decision. This contrasts with a period of 48 hours for the retention of documents obtained under reasonable suspicion powers such as section 43 of and Schedule 5 to the Terrorism Act 2000, subject to a single extension of up to a further 48 hours if an officer of at least the rank of chief inspector is satisfied that the examination is being carried out expeditiously, and that it is necessary to continue the examination to ascertain whether the document is one that may be seized.[48]

    (b) Schedule 7 contains, as the JCHR has pointed out, no express system of safeguards for categories of material such as legally privileged material, excluded material and special procedure material (including "*journalistic material*").[49]

    (c) The retention of electronic data is liable to be held for very long periods under the MOPI regime, which as I reported in July 2013 has been recently criticised in the courts.[50] The system is in marked contrast to the rules and guidance that exist under the Protection of Freedoms Act 2012 concerning the retention and use of material (including biometric material gathered from Schedule 7 detainees) for the purposes of national security.

38. It is difficult to say more about some of these issues before judgment has been given in the *Miranda* case. I note however that the Minister has undertaken in his response to the JCHR to revisit the issue of safeguards in the light of the judgment in *Miranda*, once it is available, and of any subsequent comments of the Independent Reviewer.

39. **I recommend that the Government indicate how adequate safeguards are to be provided in respect of legally privileged material, excluded material and special procedure material, and will comment further on this issue as seems appropriate after the *Miranda* judgment.**

40. **I recommend that the Government indicate how it will ensure that private electronic data gathered under Schedule 7 is subject to proper safeguards governing its retention and use.**

41. The JCHR also recommended that the Bill be amended so as to specify the intervals for the review of detention, rather than leaving them to be specified in the Code of Practice. I agree, and was pleased to note that the Government in its response of 11 November offered

[48] Counter-Terrorism Act 2008, section 5.

[49] JCHR report, fn 10 above, para 125. These concepts are defined in the Police and Criminal Evidence Act 1984, sections 10-14.

[50] D. Anderson, *The Terrorism Acts in 2012*, 10.74-10.80.

to reflect on this point. **I recommend that the intervals for review of detention be specified in Schedule 7, not simply in the Code of Practice.**

USE OF EVIDENCE GIVEN UNDER COMPULSION

42. In its decision of August 2013 in *Beghal v DPP*, the Administrative Court (Gross LJ, Swift and Foskett JJ) commented as follows:

> "It is one thing to conclude that the Schedule 7 powers of examination neither engage nor violate a defendant's Art. 6 rights; it is another to conclude that there is no room for improvement. For our part, we would urge those concerned to consider a legislative amendment, introducing a statutory bar to the introduction of Schedule 7 admissions in a subsequent criminal trial. The terms of any such legislation would require careful reflection, having regard to the legitimate interests of all parties but, given the sensitivities to which the Schedule 7 powers give rise, there would be at least apparent attraction in clarifying legislation putting the matter beyond doubt."

43. The issue was adverted to in my July 2013 report, in which I said that it was essential that answers given under compulsion should not be used in proceedings where they could incriminate the person who gave them, and stated my belief that it is generally accepted that answers given under compulsion in Schedule 7 interviews could never be used in a criminal trial.[51]

44. I have no doubt that Ministers and Parliament will wish to give the most careful consideration to the recommendation of the court. For what it may be worth, I add my voice to it and **recommend that a statutory bar be introduced to the introduction of Schedule 7 admissions in a subsequent criminal trial.** As the Court in *Beghal* recognised by its reference to "*sensitivities*", the point of this change would be not merely to confirm the position as it is already assumed to be, but to give those subject to Schedule 7 an assurance that whilst they are obliged to answer questions, their answers could not be used against them in criminal proceedings. The Code of Practice would need to provide that persons questioned under Schedule 7 are given that assurance.

CONCLUSION

45. In formulating these recommendations, I have sought to ensure that those subject to Schedule 7 examinations are given the maximum safeguards consistent with the continued productive operation of these vital powers. Properly operated, I do not believe that anything in them will reduce the efficacy of those powers, or expose the public to additional risk from terrorism.

46. Each of my recommendations goes further than anything so far proposed or agreed to by the Government. I recognise however that the proposed new thresholds will be considered

[51] D. Anderson, *The Terrorism Acts in 2012*, July 2013, 10.63-10.64.

over-cautious by those who take the view, as did the JCHR, that nothing short of reasonable suspicion should be required for the exercise of the more intrusive Schedule 7 powers. The issue is a difficult one, and I have sought to explain my caution at paragraph 28, above.

47. I have taken the opportunity in recent days to discuss my recommendations on a preliminary basis with senior police officers, who have not informed me of fundamental objections to any of them. If these proposals are translated into law, ports officers will need to be provided with all possible clarity by the new Code of Practice.

DAVID ANDERSON Q.C.
Independent Reviewer of Terrorism Legislation

20 November 2013

SUMMARY OF INDEPENDENT REVIEWER'S RECOMMENDATIONS

1. **I recommend that no change be made to the existing threshold for the exercise of the powers to stop, question and search, save for the amendment proposed in the Bill where strip search is concerned (para 19, above).**

2. **I recommend that:**

   (a) Detention be permitted only when a senior officer is satisfied that there are grounds for suspecting that the person appears to be a person falling within section 40(1)(b) and that detention is necessary in order to assist in determining whether he is such a person.

   (b) On periodic review, a detention may be extended only when a senior officer remains satisfied that there continue to be grounds for suspecting that the person appears to be a person falling within section 40(1)(b), and that detention continues to be necessary in order to assist in determining whether he is such a person (paragraph 30, above).

3. **I recommend that the power under the proposed paragraph 11A to make and retain copies of things detained pursuant to paragraphs 5, 8 and 9, should apply to personal electronic devices and to the data stored on them only if a senior officer is satisfied that there are grounds for suspecting that the person appears to be a person falling within section 40(1)(b) (paragraph 36, above).**

4. **I recommend that the Government indicate how adequate safeguards are to be provided in respect of legally privileged material, excluded material and special procedure material, and will comment further on this issue as seems appropriate after the *Miranda* judgment (paragraph 39, above).**

5. **I recommend that the Government indicate how it will ensure that private electronic data gathered under Schedule 7 is subject to proper safeguards governing its retention and use (paragraph 40, above).**

6. **I recommend that the intervals for review of detention be specified in Schedule 7, not simply in the Code of Practice (paragraph 41, above).**

7. **I recommend that a statutory bar be introduced to the introduction of Schedule 7 admissions in a subsequent criminal trial (paragraph 44, above).**

20 November 2013

Written evidence submitted by Charity Finance Group [CT 12]

Executive Summary

(i) This submission will outline how counter-terrorism legislation (specifically counter-terrorist financing legislation and sanctions regimes) has made it increasingly challenging for UK charities to transfer funds through formal banking channels to support operations abroad.

(ii) Messaging from policy makers identifying charities as organisations vulnerable to abuse by terrorists. This messaging combined with a growing risk-averse approach from banks in light of enhanced AML/CTF legislation, and the fact that many charities operate in 'high risk' regions, has resulted in growing barriers to transferring funds overseas. Problems reported include delayed payments, an inability to transfer to certain countries and the closure of MSB services.

(iii) This problem is escalating despite efforts from the charity sector to mitigate its impact. Enhanced sanctions regimes and counter-terrorism legislation mean that banks are becoming increasingly risk averse. Additionally, there is no economic incentive for banks to support charities by transferring funds – the cost of mistakes is too high.

(iv) It is therefore essential that Government takes action by supporting banks to apply proportionate risk management approaches, and working with overseas governments and regulators (including the EU, US and FATF) to ensure their activities do not hinder vital aid efforts. We would like to see Government lobby globally for an international version of the US OFAC licence, which charities could quote to allow 'safe passage' of funds for humanitarian purposes anywhere in the world.

(v) If action is not taken this problem risks destabilising wider counter-terrorism efforts: if charities are unable to use formal banking channels they will increasingly turn to untraceable, informal means to transfer funds (e.g. by transferring large amounts of cash over borders) – making them more vulnerable to abuse by terrorists. Additionally, by providing humanitarian aid and help with infrastructure building, charities have a key role in contributing to the stability of a region and thus preventing the growth and spread of terrorism abroad. There is a clear incentive for government to support this work and an imperative not to undermine the influence that humanitarian organisations can have in preventing terrorism.

1. Introduction

1.1. Charity Finance Group; inspiring the development of a financially confident, dynamic and trustworthy charity sector. Charity Finance Group works with finance managers to enable them to give the essential leadership on finance strategy and management that their charities need; promoting best practice in charity finance, driving up standards, campaigning for a better operating environment and ensuring every pound given to charity works harder - it's essential to maintain the trust of charity donors. CFG has more than 2,200 members, all senior finance professionals working in the sector and collectively our members are responsible for the management of over £19bn in charitable funds. This response was developed with input from member charities and CFG's Treasury Special Interest Group, whose membership comprises of treasurers from a number of major international charities.

1.2. Part of the stated remit of this inquiry is to '*re-examine how effective the Government is in stopping terrorist attacks*'. This response is framed around the effectiveness of Government counter-terrorism policy in the context of its impact on the UK charity sector.

1.3. In the past decade global policy-makers have increasingly identified charities as organisations which are vulnerable to abuse by terrorists. Public awareness of this fact, combined with an increasingly risk-averse approach from banks (in light of enhanced anti-money laundering (AML)/counter-terrorist financing (CTF) legislation and sanctions regimes), and the fact that many international charities operate in fragile and/or conflict ridden states, has meant that charities are finding it increasingly challenging to send money to certain countries through formal banking channels. This problem has been particularly acute amongst Muslim charities, who have more frequently reported having bank accounts closed or donations blocked.

1.4. These problems are likely to worsen unless Government addresses them. The recent withdrawal by Barclays of banking facilities from MSBs servicing Somalia, and the inability to transfer funds into Syria are recent examples of how delays and difficulties with sending funds can disrupt important work abroad.

1.5. CFG recognises that the issues raised in this submission are not solely the responsibility of the UK Government. Complex global finance structures implicate other international institutions and countries (e.g. US, EU, FATF, IMF). Banks' interpretations of the – rather than the regulations themselves – are often misguided; both charities and government charities ought to work to improve practices and engage with banks on following the regulation in a manner that doesn't undermine charitable objects. However, Government needs to take the lead in addressing these issues and the wider negative effects of CTF legislation or, we believe, the UK international charity sector and the vital work it carries about abroad (including activities which can undermine terrorist efforts) will suffer.

1.6. A number of charities and umbrella bodies have been exploring these issues; in February 2013 CFG held a roundtable meeting with these organisations to discuss some of the problems experienced as a result of the global CFT regime. CFG has also met with the British Bankers' Association, Charity Commission and members of the Disasters Emergency Committee (DEC) to discuss processing payments to Syria.

2. International charities as 'high risk' customers

2.1. Many international charities have operations that provide humanitarian assistance, healthcare, outreach and infrastructure building – all of these activities support and the stabilising and development of regions, which in turn contributes to restricting the growth of terrorist activity

abroad. Civil society plays a key – albeit secondary - role in supporting counter-terrorism efforts and this consideration should be the starting point when developing policy to prevent the abuse of charities by terrorist organisations.

2.2. In recent years there have been several high-profile incidents where charities have been used as a vehicle to enable or fund terrorist or extremist activity. This has resulted in increased public awareness of the ways in which charities can be used by terrorist organisations. While such cases are an abhorrent abuse of the charity sector and the trust it receives, it is important to remember that they are rare and affect only a tiny proportion of charities.

2.3. Efforts by the Charity Commission to detect and prevent such abuses are underway and the regulator is, rightly, an important contributor to the UK's counter terrorism infrastructure. However, this is only one of its many functions.. Greater care around messaging which has recently demonstrated a misleading constant linkage between charities and potential terrorist abuse, distorts perceptions of the sector.

3. Problems reported by charities

3.1. Cases of terrorist abuse and messaging from government and regulators and charities' presence in high risk regions have led global policy-makers to identify charities as high risk banking customers. This in turn shapes banks' risk management processes, and increasingly they are taking a particularly broad-brush approach to regulations – resulting in charities (particularly Muslim charities) experiencing problems with:

- Delayed payments;
- Transferring funds to sanctioned or high risk countries;
- Opening and keeping open bank accounts; and
- Receiving funds from certain regions.

In addition to these common problems, some Muslim charities have also reported that their donors have been warned against donating by their bank. These worrying reports, that banks are taking on regulatory functions and presenting an obstacle to charities' donor support, need to be taken seriously.

DELAYED PAYMENTS

3.2. An over-cautious approach by banks can often result in delays, sometimes of months, when processing charity payments to certain areas. For example, one charity reported that any USD payment to South Sudan is likely to be delayed due to the word 'Sudan' appearing in the payment instruction. There are no sanctions on South Sudan yet it is caught because of the sanctions on North Sudan. This is an example of a relatively simple mistake having a significant impact.

3.3. Even for large charities, with dedicated and experienced treasury teams, it can take a week or more for international transfers to reach their destination. For smaller charities, without such resources, often the delays are longer and payments simply returned.

TRANSFERRING FUNDS TO SANCTIONED OR HIGH RISK COUNTRIES

3.4. Many international charities carry out vital work in high-risk countries (that typically lack sophisticated infrastructure and regulation) ; they have a need to transfer funds to the region – either to partners carrying out work or to regional offices, in order to fulfill their charitable objects. There is a clear recognition, and acceptance, amongst charities that these payments will be subject

to enhanced scrutiny which may take longer than usual to process. They become particularly frustrated, however, when payments are blocked, without caution or reason, due to broad-sweeping risk policies, that do not take into account the charities unique status.

3.5. Sanctions regimes have exemptions in place for humanitarian payments; however these offer little security for banks who are keen to mitigate their exposure to risk, often resulting in them withdrawing their services with little or no notice. Recent cases raised by charities include:

- **Sudan:** One charity said: '[*When sending funds] to Sudan we can't buy SDG, so send EUR (or other non-dollar currencies). In the past this has worked but recently these payments are not going through with the excuse of 'sanctions' coming from the currency trader intermediary banks…*'
- **North Korea:** A number of charities are implementing programmes on behalf of the EU in North Korea, and are forced by the North Korean government to use the Foreign Trade Bank of DPRK (FTB). Earlier in 2013 the UN tightened sanctions, and the US named FTB as a sanctioned entity (due to alleged links to North Korea's nuclear programme). Since then it has been practically impossible for charities to move cash into North Korea through normal banking channels. So, despite the EU's commitment to encouraging this humanitarian work to continue, the counter-terrorism sanctions present barriers to its implementation.
- **Syria:** Here there is huge demand for humanitarian assistance – 6.8m people within Syria are in need of humanitarian assistance according to DEC statistics. Yet it is near-impossible to transfer funds into the country using formal banking channels.

OPENING AND RETAINING BANK ACCOUNTS

3.6. A number of Muslim charities have reported having a request to open a bank account refused, or their existing account closed – often without explanation. In 2012 Islamic Relief reported how the only explanation offered for a major bank suddenly closing down an account was that the bank was acting in line with its policy.

CLOSURE OF MONEY SERVICE BUSINESSES (MSBs)

3.7. The recent decision of Barclays to withdraw banking facilities from MSBs servicing Somalia is one ne of the most significant developments resulting from banks' concerns around sanctions and terrorist financing. The UK remittance market provides a valuable channel - supplementing mainstream banking routes - for individuals and charities to send money abroad, particularly to regions where infrastructure is lacking.

3.8. Until Barclays' decision many major international charities used an organisation called Dahabashiil to support programming in Somalia. 40 per cent of Somalis rely on remittances (predominantly from Somali diaspora but also from charities) and no other money transfer service has anywhere near the reach of Dahabashiil into the rural (i.e. poorest) parts of the country. There could be a devastating economic and social impact from closing this funding channel on the poorest and hardest to reach in Somalia.

3.9. We are aware that a review of the UK remittance market is currently being undertaken on behalf of DfID. We would urge the committee to review and take into account the content of the DIFD report once published.

4. The impact of banking challenges on the UK charity sector

4.1. The delays and difficulties associated with transferring funds affect charities' cash flow and have a direct impact on their ability to carry out vital humanitarian work. Ultimately not having access to adequate funds lead to delays to projects or prevents work being carried out.

4.2. Irrespective of whether payments are eventually made successfully, the amount of time spent trying to understand and solve these problems, and the associated administrative cost is excessively burdensome. When payments are delayed or blocked it is not always immediately apparent why it has happened, causing difficulties for the charity.

4.3. Charities are compelled to explore and adopt creative ways of transferring payments, when formal banking channels are closed to them. This is often convoluted and expensive .For example, one charity reported overcoming some of the difficulties by paying their partners' parent entity or head office, usually based in the US or Europe, relying on internal arrangements the partner had in place for sending these funds out. Additional administration and steps in the payment 'chain' come at a cost; this does not sit well with the public (who are, rightly, increasing their scrutiny of charitable accounting) out of concern that charities optimise value for their donations.

4.4. The closure of MSBs and heavily delayed or blocked bank payments, has narrowed charities' ability to access legitimate corridors to send money internationally. This means that charities, determined to reach their beneficiaries, will increasingly turn to insecure or even illegal means to get cash to where it is needed e.g. by taking large amounts of cash over borders.

4.5. As a general rule, charities should be supported to use formal banking channels wherever possible. Alternatives are both less traceable and less accountable and, therefore, far more likely to be open to abuse by terrorists. Although we recognise that some, particularly smaller charities, have structures better suited to transferring money using more informal networks.

5. Contributing factors

5.1. As a result of complex interplay between different international bodies, regulatory regimes, and financial institutions, the problems faced by charities with payments to aid humanitarian work abroad cannot be reduced to 'poor counter-terrorist financing legislation.' . However, in discussions with charities and banks a number of problems with the legislation have been identified, which are outlined in paragraphs 5.2 to 5.9.

MESSAGING FROM GOVERNMENT AND REGULATORS

5.2. Governments and regulators have increasingly adopted a 'zero tolerance' approach to potentially terrorist activity; a vital strategy to cutting off their activity is to disrupt and prevent their use of the financial system. This has meant that. Banks are particularly cautious after seeing the potential penalties for non-compliance; they have taken heed of the government's message, broadly conceived, and adopted tight policies when dealing with what they consider to be 'high risk' customers. For example, Standard Chartered received a £340m fine imposed by the US for breaching sanctions on Iran; consequently banks are incredibly nervous about associating themselves with any activities that could be misinterpreted as something similar to their alleged offences.

INTERNATIONAL CONTEXT

5. UK CFT legislation cannot be viewed in isolation. The majority of banks have global reach and consequently are affected by the approach and activities of the US, UN, EU, FATF (special recommendation 8 relating to non-profits is frequently cited as a problem), IMF and others. For example, all USD payments clear through the United States so any USD payment initiated outside the US, to a destination other than the US, will still be cleared through the US banking system and thus regulated in accordance with US sanctions. Similarly, banks with operations in the US have to declare and explain (to the US Securities and Exchange Commission) all transactions that they release to sanctioned entities, regardless of currency, originating or destination country. Moreover, with the majority of UK banks having operations in the US, they do not wish to upset US regulators, even if they are a UK bank remitting GBP to a US sanctioned country.

5.3. As a result of this of this interconnectivity any solution would have to be a globalforce, since UK based charities acting in complete compliance with all sanctions and regulations are impacted either directly or indirectly by sanctions regimes in place elsewhere – not only in the US and Europe. **Ideally, we would like to see the UK Government lobby globally for an international version of the US OFAC licence, which charities could quote to allow 'safe passage' of funds anywhere in the world – with the originating bank being responsible for 'vetting' the transfer (through its KYC procedures).**

AMBIGUITY AROUND SANCTION REGIMES

5.4. We understand that sanction regimes are constantly evolving and so if a particular aspect is problematic, it can normally be addressed. Humanitarian payments are generally exempt from sanctions therefore, legitimate payments by charities should not be stopped in theory. Yet, in reality, banks simply aren't comfortable with the humanitarian exemption; where there are grey areas they will err on the side of caution.

5.5. An example of this caution is evidenced when charities finance materials which fall into the 'dual use' sanctions category. For example, large scale water sanitisation, which involves procuring materials which could be deemed as dual use (e.g. drilling equipment which could also be used for oil). Pipes and pumps have also been reported as problematic as they can also be used for military purposes or in sanctioned economic activities.

LACK OF A JOINED UP APPROACH WITHIN GOVERNMENT

5.6. We know that Government departments (HM Treasury, Foreign and Commonwealth Office and Department for International Development in particular) are aware of the problems faced by charities and efforts are currently underway to examine how they can be addressed. However, this is a relatively new development and there remains an inherent tension between Government priorities. For example, DfID is currently funding DEC charities to support operations in Syria; however, for other departments the counter-terrorist financing agenda inevitably takes priority.

5.7. This is also true from an international perspective. See North Korea example in paragraph 3.5.

6. The need for Government to address these issues

6.1. Discussions with banks and regulators indicate that future trends will reinforce this risk aversion. In Syria, one of the most pressing humanitarian situations, the sanctions regime is likely to get more complex. From a charity perspective, it is expected that the problems experienced with international payments will worsen.

6.2. Charities and sector bodies are starting to engage with banks and other decision makers on these issues however, at present these discussions too often, run into stalemate. The banks' priority is, understandably, to ensure that they do not fall foul of sanctions and legal obligations. Advice from lawyers suggests that there is nothing explicit in sanctions legislation to prevent legitimate charity payments from being processed. Government echo this sentiment, suggesting that decisions around processing payments are commercial choices that the bank must make and therefore outside their scope of influence. The government are therefore, the most capable party of alleviating this tension.

6.3. At present there is simply no economic incentive for banks to invest time and effort into checking and processing 'high risk' humanitarian payments. The fees they earn from charity transfers are dwarfed by the possibility of significant penalties and reputational damage if mistakes are made. It is somewhat inevitable that banks do not want to take 'risks' with charity payments and a reasonable reaction for banks to have in the current regulatory environment.

6.4. CFG, the BBA and others have been looking at individual 'problem' countries and issues such as those covered in Section 4. However, these issues also need to be addressed by Government – who are able to engage and influence global stakeholders such as FATF, US, EU – in order to find a long-term, sustainable solution that ensures that legitimate humanitarian payments are able to get to the areas where they are needed.

6.5. We recognise that this is only one small aspect of counter-terrorism efforts. However, the need for a proportionate and risk-based approach should characterise the Government's strategy as a whole. If counter-terrorism efforts threaten humanitarian work that responds to pressing human needs and even contributes to eradicating terrorism – then they are simply not effective and undermine the role that international charities play in forming strong and stable societies.

Charity Finance Group
September 2013

Written evidence submitted by Privacy International [CT 13]

Whether the Government has the capability to examine and combat the use of communications (including via the internet) in terrorism-related activities.

1. Yes.

2. We below note a separation between capability, and institutional ability to use such a capability effectively. Privacy should not rely on State incompetence or disinterest.

Whether the UK has sufficient capability to detect, investigate and disrupt terrorist threats.

3. The UK has sufficient capability to detect, investigate and disrupt threats, but a lacks adequate capability to protect innocent citizens from the side effect of intrusion. There is a lack of clear legal framework over how these powers are used, and what rights individuals have to know about and question their use. Such a clear legal framework would also allow for an independent authorisation for surveillance.

4. More explicitly, the UK does lack sufficient capability to detect, investigate and disrupt institutional thinking that threatens civil liberties and the values of the UK. The UK has an independent reviewer of terrorism which substantially depoliticised terrorism laws; why not an independent reviewer of civil liberties? We need an institution that is separate from politics, is able to comprehend modern technologies and capabilities, with a mandate to protect civil liberties.

5. Legacy of the Communications Data Bill

6. When advocating for the Communications Data Bill, the Home Office made a number of arguments that the UK lacked capabilities to deal with serious crime, paedophiles, and terrorism.[1][2] Since the work of the Joint Committee on the Draft Communications Data Bill committee concluded, it has become increasingly evident that the explanations given to both committees of the capabilities available to law enforcement and especially the Counter Terrorism Agencies were critically lacking, to the point of potentially being misleading[3][4][5].

7. The Home Secretary's refusal to allow the Intelligence Agencies to give evidence to the Joint Committee[6] looks founded in continuing institutional secrecy, with the result that two Committee of both Houses was left with an inaccurate impression by the Head of the Office

[1] Theresa May, HC Deb, 8 January 2013, c166. http://www.theyworkforyou.com/debate/?id=2013-01-08b.166.0
[2] "Track crime on net or we'll see more people die. Warning to Nick Clegg on terrorists, crooks and paedos." The Sun, 3rd December 2012 http://www.thesun.co.uk/sol/homepage/news/politics/4678082/Track-crime-on-net-or-well-see-more-people-die.html and http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf
[3] https://www.privacyinternational.org/blog/surveillance-times-have-changed
[4] http://www.independent.co.uk/news/uk/politics/exclusive-uks-secret-mideast-internet-surveillance-base-is-revealed-in-edward-snowden-leaks-8781082.html
[5] http://www.theguardian.com/uk/gchq
[6] Theresa May, Oral evidence to the Joint Communications Data Bill Committee , Q1157

of Security and Counter Terrorism.[7] Of how many capabilities revealed this summer, those directly relevant to their Terms of Reference, were the Committees informed? [8]

8. The legislated remit of Agencies is substantially different to the rhetoric used for the Bill's support,[9] for example around "economic well-being", which can be interpreted incredibly flexibly (yet did not appear in the Communications Data BIll debates) - in short, "Terrorists should be priority, not commercial rivals".[10] In light of this discrepancy, resources may have been diverted from counter-terrorism efforts, on a priority basis not considered by Parliament.[11]

9. During the deliberations over the Draft Communications Data Bill, the Home Secretary argued that it was simply metadata that was being collected, and not content. Recent revelations about metadata processing in the US has been treated with much greater concern, both domestically and internationally, being cited in the cancellation of a State Visit to the US[12], partially as a result of metadata derived surveillance of the President-Elect of Brazil.[13]

10. We are in urgent need for a general recognition of the sensitivity of metadata (beyond agencies who very much recognise the sensitivity). Every transaction we make in modern society generates metadata. For instance, it is now routine for organisations to request donations online, be they political contributions, or in support of a civic campaign. Emailed receipts will contain information within that is politically sensitive -- the size of donations or type of causes, for example. Equivalent surveillance outputs, from the same social network analysis tools as used to target the Brazilian President-Elect, would immediately produce such information of interest to the Intelligence Agencies.[14] Companies are required to surrender the communications data fed into such tools - "communications data is about the who, when, where, and how", as the Home Secretary says[15].

11. We note that while the Internet companies (Yahoo, Google, Facebook, Twitter,[16] LinkedIn, Dropbox, et al) have been quite public about their interest in protecting the privacy and rights of their users against widespread government access requests, the telephone providers have been silent about any steps they have taken to protect the privacy of UK citizens. The Communications Data Bill was replaced with a voluntary programme of work by the Home Office with the telephone providers (Vodafone, EE, O2, 3, BT, TalkTalk, et al) to look at IP address resolution. The suggestion of the next generation IP addresses (IPv6) would provide individual addressing per device continues to be valid.[17] If the committee receives oral evidence from the mobile telephone companies, we hope they would be willing to put on record a justification for their reluctance to take a (small)

[7] Charles Farr, Oral evidence to the Joint Communications Data Bill Committee, Q18 http://www.parliament.uk/documents/joint-committees/communications-data/Oral%20Evidence%20Volume.pdf
[8] http://www.bigbrotherwatch.org.uk/home/2013/07/5496.html
[9] Theresa May, Q1158 & Q1159, Joint Committee Oral Evidence
[10] http://www.theguardian.com/uk/defence-and-security-blog/2013/jul/01/gchq-nsa-eu
[11] http://www.independent.co.uk/news/uk/home-news/uks-gchq-blamed-for-cyber-attack-on-belgian-telecoms-company-8830123.html
[12] http://ojornal.com/portuguese-brazilian-news/2013/09/us-brazil-tensions-rise-after-new-spy-report/
[13] http://edition.cnn.com/2013/09/17/world/americas/brazil-us/index.html
[14] http://www.washingtontimes.com/news/2013/sep/2/us-brazil-tensions-rise-after-new-spy-report/?page=all
[15] Q1145
[16] http://www.uscourts.gov/uscourts/courts/fisc/misc-13-03-order-130913.pdf
[17] https://blogs.akamai.com/2013/06/world-ipv6-launch-anniversary-measuring-adoption-one-year-later.html#more

technical step to meet the Home Office's stated national security need, a step which does not impinge on wholly innocent individuals or require new and large publicly funded databases and interconnections. The internet companies have done the preparatory work, it is the telecoms companies who are preventing resolution of what the Home Office claim is a critical national security issue. We do however appreciate that it is difficult for the phone companies to speak on steps they refuse to take, in line with their refusal to publish a transparency report.[18]

Safeguards are ineffective

12. There was a large amount of debate beyond the Communications Data Bill Committee about safeguards. Safeguards have been shown to be fundamentally ineffective: absent confidence and evidence to the contrary, safeguards will be circumvented. Transparency and integrity are required. Currently, the UK has neither and is well behind international standards that include judicial authorisation, intercept evidence used in courts, limitations in law on collection and use, transparency and notification regimes, and rights of redress.

Mobile telephones and Policing

13. Innovations in technology have provided the state with powers of surveillance previously unimagined. Police and security agencies are now capable of directly conducting mass surveillance, and targeted invasive surveillance, without the need of interacting with any third party. It remains unclear what legal framework governs these activities. For instance, we are concerned that the Metropolitan Police has begun routinely duplicating all data off a cell phone of a suspect irrespective of charge.[19] This mass interrogation of individual's call history, contacts, messages and the other material held on a modern mobile device. The rules on the use, retention and distribution of such material are secret, and without adequate public scrutiny, are quite likely to be of concern when publicly examined.

14. Similarly, the indiscriminate use of mobile phone surveillance through the deployment of police-controlled base stations appears to be unregulated. All attempts to identify the rules under which these 'IMSI catchers'[20] [21] (aka IMSI grabbers) are used by police have been unfruitful as the authorities claim that disclosing anything about their use would hinder the prevention of serious crime and protection of national security.[22]

15. In this respect, little has changed in the security debate since the Intelligence Services Act 1994, which put GCHQ on a legal footing.[23] We look forward to working with

[18] unlike the internet companies: https://www.google.com/transparencyreport/ , https://transparency.twitter.com , https://www.facebook.com/about/government_requests, http://help.linkedin.com/app/answers/detail/a_id/41878, http://info.yahoo.com/transparency-report/, http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/, et al

[19] http://www.dailymail.co.uk/news/article-2146244/Privacy-row-Met-Police-text-email-data-ALL-suspects-mobile-phones-regardless-charged.html

[20] http://en.wikipedia.org/wiki/IMSI-catcher

[21] https://www.privacyinternational.org/media-articles/moscow-metro-says-new-tracking-system-is-to-find-stolen-phones-no-one-believes-them

[22] for example https://www.whatdotheyknow.com/request/imsi_catcher_guidance

[23] Chris Mullin, – Intelligence Services Bill [Lords], col 124, Standing Committee E, 1994. Available at https://www.privacyinternational.org/sites/privacyinternational.org/files/page-attachments/intelligence-services-bill-commons-committee-1994.pdf

Parliament identifying the areas where greater scrutiny, protections, and oversight are required.

Sam Smith
Privacy International
September 2013

Written evidence submitted by
Google, Facebook, Yahoo!, Twitter and Microsoft [CT 14]

Mutual Legal Assistance Treaties

1. We (the representatives of Yahoo!, Facebook, Google, Twitter and Microsoft) write to the Committee with evidence regarding the second point in its terms of reference: *"The effectiveness of the Government in working with foreign Governments and Multi-lateral organisations to counter terrorist threats at home and abroad."*

2. We firmly believe that reforming, and further investing in, the well-established Mutual Legal Assistance Treaty ["MLAT"] system is the appropriate means by which UK law enforcement should seek data to support criminal investigations. The MLAT system mirrors the international and multi-jurisdictional nature of the internet, respects national sovereignty, and ensures appropriate respect for user rights. Efforts should be made to improve these well-understood and judicially respected MLAT processes before the UK considers further legislative changes.

3. Although doubts have been expressed as to whether MLAT reform is the right route for better access to data held by communications providers under US jurisdiction, those concerns find no support in the text of the UK-US MLAT. Indeed, the treaty's introduction makes clear that the UK-US MLAT applies to "*investigation, prosecution, and combatting of crime through cooperation and mutual assistance in criminal matters . . ." See, also, the definition of "assistance" in Article 1, Par. 2 and the definition of "proceedings" in Article 19.*

Ways to improve the MLAT process

4. MLAT is a government-to-government process. The providers to whom disclosure requests are made do not have detailed insights into its operation 'from the inside'. We can, however, provide observations based on our engagement with the process and with public officials who administer it.

5. Our experience indicates that the following areas merit further investigation:
    a. Differential treatment of disclosure requests (e.g.: how law enforcement agencies ["LEAs"] prioritize urgent requests).
    b. Impact of high volumes of requests for minor offences (e.g.: parking fines) and the potential benefits of UK LEAs deprioritising such requests.
    c. Levels of expertise and knowledge within UK LEAs about how to submit a complete and compliant request to US providers (including meeting the relevant US evidence standards).
    d. Existence of consistent guidance (including pro-formas) from both the UK and US authorities to assist requesting agencies.
    e. Resourcing levels in both UK and US agencies that handle requests (including reimbursement of costs between UK and US authorities).
    f. Relationship between length of the process and costs to both sides, and the extent to which inefficiencies can be reduced.
    g. Potential benefits of a model MLAT implementation method (similar to the one used among EU member states).

h. Agreement on timetables for response by governments and providers to ensure that MLAT processes respect privacy, investigative, and judicial needs.
i. Effectiveness of safeguards to prevent misuse of the MLAT process and public resources.
j. Awareness of any agreed protocols outlining the offences for which communications data can be requested by UK LEAs from US providers via MLAT.
k. Incidence and frequency of training for LEAs, government officials, judicial authorities, providers and others involved in the MLAT process (on both sides). This should include training about the privacy considerations inherent in MLAT requests.

6. This list is not exhaustive and must of course be supplemented by the experience of the Home Office and requesting UK LEAs, as well as the US authorities concerned. We believe, however, that with action in each of these areas, existing MLAT process could be reformed to recognize important privacy and law enforcement interests without the need for wholly new legislation.

7. We therefore recommend that the Home Office prioritise work to reform and improve the MLAT process.

8. We also recommend that requests for user data made by the UK Government are made as transparent as possible. Each of our companies already publishes a transparency report[1] and, as public concern grows around the world about the scale of digital surveillance, we believe that greater transparency is important in encouraging a full public debate and maintaining confidence that powers are not being abused.

Emma Ascroft, Director Public Policy, Yahoo!

Becky Foreman, Head of Government Affairs, Microsoft UK

Theo Bertram, Public Policy Manager, Google

Sinead McSweeney, Director Public Policy EMEA, Twitter

Simon Milner, Director Public Policy UK and Ireland, Facebook

October 2013

[1] Please see here for further details: Google's report can be found here: http://www.google.com/transparencyreport/ ; for Yahoo! it can be found here: http://info.yahoo.com/transparency-report/uk/ ; for Facebook it can be found here: https://www.facebook.com/about/government_requests ; for Twitter it can be found here https://transparency.twitter.com/ and for Microsoft it can be found here: http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Written evidence submitted by the Charity Commission [CT 15]

Introduction

1. Concerns about a charity being abused for terrorist purposes corrodes public trust and confidence in charities. The number of cases where it has been proven that charities or individuals closely connected with them have been involved in supporting terrorist activity is small in comparison to the size of the charity sector. Nevertheless, any abuse of charities for terrorist purposes is completely unacceptable. We believe that the Charity Commission's ("the Commission") work, in partnership with the Home Office, police, the Security Service and other agencies involved in counter terrorism efforts, is making it harder for terrorists to abuse charities and obtain funding through charity donations.

2. There are over 350,000 charities in England and Wales of which over 163,000 are registered with the Commission. The total annual income of registered charities is £60 billion. Many of these charities are very small; 69,000 have an income under £10,000. The vast majority of charities are carrying out legitimate work and are not at risk of terrorist abuse. But some are at risk - of their funding being diverted for terrorist purposes or of charity personnel using the charity as a cover for travelling overseas for terrorist training or for raising funds. There have been two recent criminal court cases specifically involving fundraising for terrorist purposes in the name of charity.

How Charities Might Be Abused

3. There are number of ways in which charities can be vulnerable to abuse for terrorist purposes. FATF, the international governmental body which sets standards for combatting terrorist financing, in its Recommendation 8, says:

   "Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

   a) by terrorist organizations posing as legitimate entities;

   b) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and

   c) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations"[1].

4. In the Commission's experience, there is a risk that funds may be raised in the name of "charity" generally or under the name of a specific charity but the collectors use it to support terrorist activities, with or without the charity's knowledge. It is also possible, although hard to prove, that charities might be set up as a sham (either here in the UK

[1] Financial Action Task Force: Best Practices: Combating the Abuse of Non-Profit Organisations (Recommendation 8) http://www.fatf-gafi.org/documents/guidance/bpp-npo-2013.html

or abroad to receive funds from the UK), the purpose of which is really to raise funds or use its facilities or name to promote or carry out terrorist activity.

5. A charity's name, status and assets are potentially at risk of abuse. Charity vehicles may be used to transport people, weapons or terrorist propaganda, or charity premises used to store them or arrange distribution. Individuals supporting terrorist activity may claim to work for a charity and trade on its good name and legitimacy to gain access to a region or community, or use it as cover to travel to hard to reach places where, for example, they attend terrorist training. A charity's communications network could be exploited to allow terrorists to contact or meet each other, and charity premises may provide the opportunity for terrorists to meet. Terrorist activity may be hidden or take place alongside legitimate charitable activity. There have also been occasions when terrorists, and those with extremist views who encourage and support terrorism and terrorist ideology, have used charity events to make those views known, or have used charities to promote or distribute their literature.

6. Sometimes it is the partner organisations the charity works with and funds that may be supporting inappropriate activities, and the charity becomes tainted as a result. These risks increase if the charity's financial, due diligence and monitoring controls are weak. Similarly, the charity's beneficiaries may use the money they have been given by the charity for terrorist purposes.

Extent of the risk and evidence of abuse

7. The number of cases where there has been sufficient evidence to prove charities have been involved in supporting terrorist activity whether directly, indirectly, deliberately or unwittingly is very small in comparison to the size of the sector. Nevertheless the Commission has come across cases from a regulatory perspective where it is concerned that charities have supported terrorist activities and/or charitable funding may have been diverted to support terrorist purposes, but it has been difficult to prove. In some cases, we have found deficiencies in a charity's due diligence procedures, and the failure to properly document, monitor and verify the use of charitable funds, including by its partner organisations and other agents acting for the charity, particularly overseas. This has prevented trustees from demonstrating that those funds have been used legitimately and properly and in accordance with furthering the charity's objects.

8. There have not been many convictions for terrorist financing involving charities. On 2 August 2012, twin brothers Mohammed and Shafiq Ali were convicted of raising money to fund terrorism and sentenced to three years imprisonment by the Central Criminal Court. They undertook street collections purportedly for charity. They pleaded guilty to raising £3,000 which they sent to a family member in Somalia for terrorist training/fighting. On 21 February 2013, Ashik Ali, Ifran Khalid and Ifran Naseer were convicted at Woolwich Crown Court of committing acts in preparation for terrorist attacks – the particulars of the offence included collecting money for terrorism. They raised funds by fraudulently presenting themselves as charity fundraisers using high visibility vests and collections buckets bearing the name of the charity Muslim Aid; only £1,500 of the £14,000 raised reached the charity. A licenced collection in the name of Muslim Aid

took place for one day, however the individuals (and others) continued to raise funds on consecutive days unlawfully and without the charity's knowledge or consent

9. There are challenges and risks for charities delivering aid and humanitarian relief in areas of conflict overseas. Over the past few years we have seen an increasing number of charities and organisers of charitable appeals raising funds for humanitarian assistance overseas, and charities organising convoys and shipments of aid by road overland from the UK to Syria and other areas affected by conflict. As well as relief goods and medical equipment in these shipments, cash may also be carried. Although charities sometimes take large amounts of cash overseas, there are significant risks with this. The use of cash couriers is a method which has also been used to move funds for terrorist purposes. Cash smuggling is also one of the methods used by terrorist financers, money launderers and organised criminals to move money in support of their activities. It is for this reason that the Commission has published regulatory guidance which strongly advises charities, their trustees, employees, volunteers and representatives against moving significant amounts of cash from one location to another on their person or in personal luggage.

10. We have advised charities that carrying large sums of cash in person, unless supported by appropriate documentation, is likely to be viewed suspiciously by ports and police officers and may be subject to seizure under the Proceeds of Crime Act – and ultimately lost to charity. The Commission is aware of instances of charity representatives leaving the UK for overseas with large amounts of cash which has been seized by customs officials because the individuals concerned were not able to evidence the origin of the money or its intended purpose. The Commission has therefore published regulatory alerts for trustees warning them that if they carrying cash they also need to be aware of and comply with the legal requirement to declare cash to HMRC when leaving or entering the UK, currently above a threshold of 10,000 Euros, and that failure to declare or account for the money may lead to seizure of the cash at the port or airport of departure by the UK Border Agency.

11. Over the last year, there have been high operational risks for charities working in Syria and surrounding countries in the humanitarian aid effort. This has been difficult partly because of the imposition of financial sanctions and the limited availability of banking services there which means charities are more reliant on moving funds using Money Service Businesses, Informal Value Transfer Systems and/or by moving cash. There have also been concerns about charities being able to ensure that work delivering aid and relief on the ground through local partners is effective and only used for legitimate purposes, given the challenges in carrying out due diligence checks on local partners and being able to monitor and verify the end use of funds to ensure that aid is reaching the intended beneficiaries.

Reducing the ability of terrorists to abuse charities

12. The Commission is not a prosecuting authority and does not conduct criminal investigations. Where there are concerns about suspected terrorist abuse connected to a charity, the Commission will always liaise with and work closely with the police and the Security Service as terrorist activity is a criminal offence. However, the

Commission does have a role to play and its approach in tackling this kind of abuse is to supplement both the criminal, financial sanctions and terrorist asset freezing regimes through regulatory oversight by the Commission and the charity law framework.

13. Examples of the types of issues the Commission conducts investigations and enquiries into include concerns about money the public has given to a charity not reaching its destination and being diverted, concerns about extremist speakers at charity events, and charity partnerships with designated organisations or individuals thought to support terrorists, here and overseas. The Commission monitors charities of concern and carries out inspection visits where necessary. For example, in one case, we identified a charity whose website hosted inappropriate material. Our engagement resulted in the charity removing those webpages from its website – it contained a list of 'martyrs' including a number of suicide bombers.

14. Charity is a legal status and being registered as a charity is not a license to operate. Therefore, the Commission's role in combatting terrorism is important and steps need to be taken to stop non-compliance and abuse in the sector. The Commission's ability to close down a charity that may be or has been abused for terrorist purposes is very limited. However, if it could be shown the purpose of setting up a charity was to support terrorism, even if it had ostensibly charitable purposes, this would not be a charity in law; it would be a sham. If it could not be evidenced that the organisation was a sham or had collateral terrorist purposes, but there was evidence that an individual within a charity, for example a trustee, was involved in terrorist activity or supported or promoted terrorism, this would raise regulatory concerns about their suitability to continue to be involved in the charity.

15. The Charity Commission's published counter-terrorism strategy, complementing CONTEST, describes the Commission's role and approach to dealing with concerns about the abuse of charities for terrorist purposes. The strategy has a four strand risk–based approach:

    Awareness - raising awareness in the sector to build on charities' existing safeguards

    Oversight and Supervision – proactive monitoring of the sector, analysing trends and profiling risks and vulnerabilities

    Co-operation – strengthening partnerships with government regulators and law enforcement agencies both nationally and internationally

    Intervention – dealing effectively and robustly when abuse, or the risk of abuse, is apparent

16. We place a strong emphasis on prevention and giving regulatory advice and guidance to charities to stop abuse in the first instance. We have published an online

toolkit *"Protecting charities from harm"*[2] which includes chapters on *"Charities and terrorism"* as well as on "*Due diligence and monitoring and verifying end use of funds"*, on *"Holding, moving and receiving funds in the UK and internationally"* and more recently on *"Protecting charities from abuse for extremist purposes and managing the risks at events and in activities"*. We produced the toolkit in consultation with charities and counter-terrorism agencies. This is a core part of the *Awareness* strand - raising awareness of risks and vulnerabilities, setting out the legal duties and responsibilities of trustees and expectations of standards to be met and providing them with practical tools to manage the risks.

17. The Commission also publishes and disseminates regulatory alerts and warnings about particular risks, and issues "safer giving" advice for the public, and "safer collecting" advice for charities. The latter was specifically issued in response to the January 2013 fundraising convictions referred to above. We issued safer giving alerts during key humanitarian disaster appeals and important religious festivals, such as our recent Ramadan safer giving campaign and at Christmas.

18. Since October 2012, we have carried out 21 outreach events with the sector on a range of subjects, including sending money to and operating in high risk areas overseas (e.g. Syria and Somalia), on managing extremism risks associated with speakers and publications, and on charitable fundraising and collections. Feedback indicated that 82% of those who attended said that they were better prepared after the event in knowing how to handle extremist speaker issues.

19. These actions help to build sector awareness and knowledge and give trustees access to a range of practical tools to help them manage the risks and strengthen their charity's safeguards against terrorist abuse.

Co-operation with law enforcement

20. There is no doubt that the Commission's effectiveness in this area depends on effective, strong relationships with other law enforcement and counter-terrorism agencies. These relationships are good but we realise it is important to make sure they continue to develop and strengthen. We have undertaken work to enhance joint working between the Commission and the law enforcement and intelligence community. This includes a close relationship with the police, both in the Metropolitan Police Service Counter Terrorism Command, and in the regional counter-terrorism units. We also have strong links and regular liaison with the Security Service. This ensures that our work, where appropriate, is intelligence led and allows us to take action to disrupt those that seek to exploit charities for terrorist ends. We always work closely with the police and other counter terrorism agencies where there are suspicions of terrorist abuse involving charities. We also assist the police and other agencies with their own investigations where a charity is connected to it.

[2] Protecting Charities from harm: Compliance toolkit: http://www.charitycommission.gov.uk/detailed-guidance/protecting-your-charity/protecting-charities-from-harm-compliance-toolkit/

21. Our co-operation with law enforcement and other agencies is enhanced through the ability to exchange information through the legal gateway under sections 54 - 56 of the Charities Act 2011. In 2012-13 there were 155 counter-terrorism related information exchanges disclosures. 106 of these were from the Commission to other agencies and 49 were disclosures from other agencies to the Commission.

22. In 2012-13 the Commission conducted 32 regulatory cases which involved terrorism related issues, some of which resulted in or involved inspection visits to the charities concerned.

The international dimension - working with other governments on investigations

23. In the Commission's view, monitoring and supervision at an international level can only be effective if there is good collaboration between regulators, law enforcement agencies and security agencies. This can present challenges. In some cases links with other countries may not be strong.

24. There are well established mechanisms for international exchanges on criminal issues through the Mutual Legal Assistance Treaty (MLAT). On money laundering, countries' Financial Investigation Units (FIU's) collaborate through the Egmont Group. For charity regulators, in some countries there is not always a specific regulator of the not for profit sector to liaise with, in some cases there are multiple Ministries who have an interest and even if there is a regulator, they may not be seen to have a role in counter terrorism issues. Information exchanges can be difficult from a legal perspective where the regulator in another country is a tax authority.

25. In terms of information sharing, the Commission generally makes more disclosures through our domestic statutory legal gateway to other countries' regulators than it receives.

The international dimension - supporting other governments and multi-laterals

26. Internationally the Commission has worked closely with the United Nations, a non-profit organisation (NPO) called the Center on Global Counterterrorism Co-operation, Canada and other countries in a global programme encouraging greater awareness and international cooperation to counter the risk of financial and terrorist abuse of the non-profit sector. This involved co-organising a series of regional workshops beginning with a global meeting in London in 2011 followed by five regional conferences in South East Asia, Asia Pacific, Sub Saharan Africa, the Gulf and South America. The workshops have advised governments by providing technical expertise and support, for instance on effective registration, reporting and monitoring of charities as well as investigating terrorist abuse involving charities and other NPOs. The Commission's contribution was led by its International Programme. The work resulted in a report which was published in June 2013[3].

[3] http://www.globalct.org/publications/to-protect-and-prevent-outcomes-of-a-global-dialogue-to-counter-terrorist-abuse-of-the-nonprofit-sector/

27. On behalf of the UK Government, the Commission's International Programme is also co-chairing with the Canadian Government a global study on terrorist abuse of the NPO sector. The work will be presented to the FATF in June 2014, and early indications suggest that terrorist abuse of the charity sector takes place in all regions of the world, with governments often lacking the tools to identify, investigate and prosecute such abuse.

28. The UK is more widely a leading partner of technical assistance to other countries through the Commission's International Programme. It supports governments in other countries who wish to do so to develop effective, proportionate regulation that allows charitable bodies in their jurisdictions to flourish and that helps to prevent and to tackle abuse. Support comes in the form of workshops, training sessions and technical advice and we promote models of good practice in proportionate regulation. The Commission's investigators have also provided training to some other governments' regulators, law enforcement agencies and FIU's. We have worked with governments in the Gulf, including Qatar, Kuwait, Bahrain, the United Arab Emirates and Saudi Arabia, in Pakistan and Indonesia, and in Africa, in particular in Kenya and recently in South Africa. Many charities in England and Wales work and spend money internationally often through not for profit organisations, therefore there is a real interest and importance from a UK perspective in good charity governance internationally.

29. The Commission's International Programme, until June 2013, was funded by the FCO. Its future is dependent on securing funding for it to continue its work.

Money Service Businesses

30. There are several methods of moving funds other than through formal banking methods, including Money Service Businesses, which charities may use to hold or transfer funds to a particular region and pay over on the charity's behalf. Our guidance[4] strongly advises charities to use formal banking systems to ensure that charity funds are safeguarded, and that appropriate audit trails are produced of the sort that trustees must keep for the receipt and use of money. However, we do appreciate that charities may in some circumstances need to use alternative financial systems to hold or move the charity's money, particularly where banking services are limited or non existent, such as in areas with poor infrastructure or in areas of conflict and/or subject to complex emergencies. These methods are, however, more inherently risky than traditional banking methods and, therefore, trustees need to ensure that these risks are mitigated and appropriate safeguards are in place.

Summary

31. The Commission believes that through implementation of its strategy for dealing with the risk of and concerns about the abuse of charities for terrorist purposes, in

[4] http://www.charitycommission.gov.uk/detailed-guidance/protecting-your-charity/protecting-charities-from-harm-compliance-toolkit/chapter-4-holding-moving-and-receiving-funds-safely-in-the-uk-and-internationally/

particular, its regulatory work investigating and monitoring charities and its outreach and prevention work with the sector, it has been made more difficult for terrorists to abuse charities and divert charitable funds.

32. There is, however, more the sector can do itself to strengthen safeguards and controls in charities and to manage the risks of terrorist abuse. As regulator, we do need to balance work in this area with other statutory regulatory responsibilities that we have, but there is, subject to resourcing and capacity restraints, more that the Commission could do. We have made suggestions as to how the Commission's regulatory powers can be strengthened to deal with different kinds of charity abuse, including terrorist abuse. For example, to widen the range of offences and events that trigger automatic disqualification as a trustee – currently, money laundering and terrorist offences do not disqualify someone from acting as a trustee. We have also fed into the work of the Extremism Task Force. The Commission remains committed to prioritising strong enforcement action in cases where there is suspected terrorist abuse, through investigations and monitoring of charities of concern and continued effective close working and collaboration with other counter-terrorism agencies in the UK and internationally. It is also important for us to continue, through our outreach and other prevention related work, to raise awareness of trustees' legal duties and what charities themselves can do.

33. Finally, we do need to be alert to the fact that risks for charities from terrorism will inevitably change and evolve over time. It is likely that terrorists will continue to find different ways to exploit charities and their activities for terrorist purposes,, for example through internet messaging, the abuse of digital currency exchanges and internet and mobile payment and transfer systems. We need to make sure that we respond to these changing risks.

The Charity Commission for England and Wales
October 2013

Written evidence submitted by Roger Bennett [CT 16]

I am writing as a private individual. I am aware that the deadline has passed. The committee may still wish to consider this short submission. The submission consists of only 10 short paragraphs. The submission is made by a citizen rather than an organisation. If the committee decide to consider the submission then I believe that it should not be published due to (a) its late arrival, as I only became aware of the work of the committee yesterday, and (b) and my status as an individual rather than an organisation or politician.

I am now retired having worked for the Fire and Rescue Service between 1978 and 2010 where prior to retirement I held a senior role as Corporate Head of Civil Contingencies and Resilience. I operated at GOLD command level, and passed a Strategic Assessment and Development Centre prior to securing my Strategic role in the Fire and Rescue Service.

I have a First Class honours degree (BSc Hons) in Fire Engineering and Management from the University of Central Lancashire, and a social and economic science Masters degree (MSc Econ) in Strategic Studies from the Department of International Politics at the University of Wales Aberystwyth, where I took the Michael MccGwire prize. I have a keen interest in people behaviour, with several articles published about human behaviour in fire and a dissertation that covered amongst other things 'insider outsider groups'.

(1) It doesn't matter what decisions are made by a government or any of its agencies; if that or those decisions preserve life.

(2) The preservation of life must be the fundamental principle upon which everything evolves. I understand the 'Right to Privacy' and the right to a private life, and I recognise that this 'right' is embedded in the Human Rights Act. However, I still take the far reaching view that the 'Right to Life' is of the primary importance. It does not matter how well society is performing economically, how good the health care system is, or how good the education system is, or how good the transportation systems are; if you are not here to enjoy these provisions or to enjoy the strong performance that underpins a thriving society.

(3) I would not even go as far as to say that the 'right to a private life' should be balanced with the needs of the State. Indeed, any 'right to a private life' must be discarded if such a 'right' prevents or hinders the State from preventing its citizens from being violently murdered while going about their lawful business on the streets, in public venues, and on the transportation systems.

(4) You may have noticed that I have preferred to use the words 'murder' and 'murderers' rather than 'terrorists' and 'terrorism'. This is because there are certain connotations that can be assigned to the latter words. This includes some perverse assignation of a perceived ideological status. The failure to use appropriate language and to avoid inappropriate language is madness on our part. Those who set off bombs, or take weapons to an event, deal in death and have a clear intention

to murder. We should hinder their attempts to somehow elevate their cause or elevate their status within the wider public domain. Their intention is not to injure or to maim, their intention is to indiscriminately commit murder, and to do so, on as wide a scale as possible. Given the odious nature of their intention, why do we use language that strengthens their purpose?

(5) I find it strange that we still treat these murderers and potential murders with kid gloves. We allow our media to widely, and accurately, and succinctly, inform others of the methods, tactics, and strategies of our enforcement agencies. We provide detail about our surveillance systems. We provide that explanation to the extent, that we even explain that which works and that which is a bit more difficult for us to use. It simply beggars belief that we as a society do very little to protect our fellow citizens while paradoxically we arm the murderers by informing them of our information gathering systems. 'Counter-terrorism' must be one step ahead of the murderers, but we somehow allow ourselves to hold their hand so that they can keep up with us. To do so, is simply madness, but nevertheless that is what we do.

(6) We do not adequately protect our systems and surveillance 'weapons', and we do not adequately punish those that make the choice of betraying us.

(7) So what changes do I propose? Well the first one is for someone to begin considering how 'language' can and does impacts on others. What language could hinder the wider gains that the murderers try to achieve. What language could reduce the potential for marginalisation of individuals. What language should be used when there is a specific threat. What language should be used following an event. And for central guidance to be provided that informs others of the language that should be encouraged throughout. This equally applies to wider situations e.g. influenza pandemic, a major natural catastrophe. The consistent use of appropriate language can be a powerful weapon. I expect that we spend billions on actual weapons and systems and people, but very little if nothing on a language strategy. This therefore is the first of my two big hits for the Committee to consider.

(8) The second hit is about electronic surveillance. We should continue to work with partners to develop electronic surveillance systems e.g. emails, mobile phone data, internet message boards or whatever. This continual development should be far reaching, worthwhile, and should become an even stronger tool in the armoury of the 'Counter-terrorism' agencies. There should be no 'right to a private life' when it comes to preventing our citizens from becoming victims of a violent murder. But there should be a caveat, and maybe this is where the 'balance' comes in. Under no circumstances whatsoever can any information that is obtained, then be used by any agency or to bring about any prosecution that is NOT 'Counter-terrorism' related. If you got the information from for example, reading an email, well enjoy the read, because unless we are dealing in death, then the information cannot be used. The HMRC for example, cannot use the information. Indeed if it could be shown that an agency instigated a separate non 'Counter-terrorism' investigation purely on the grounds of the email detail, then that outcome of that investigation should also become void in law. By providing this safeguard to the use of information, we bring about the 'balance' that society probably expects and is certainly entitled to. We will

do much more to gather information, we will do much more to make good use of that information, but we will restrict how that information is used. The information can only be used for the purpose of 'Counter-terrorism', and we will prevent it from being used for anything else or for being used as a catalyst to begin other investigations. The information that we obtain has been obtained to prevent or to reduce the potential of death, it cannot be used for any other sole purpose. Yes, that information must still be shared with all agencies to ensure 'joined up working' but it is its use that is limited.

(9) Finally, we will severely punish those that betray our country. If you choose to divulge secrets, then you must expect to be treated as a spy. Spies come in many forms, it doesn't matter if you are the Editor of a newspaper, the writer of a Blog, an analyst, a soldier, or a government employee. If you make a conscious decision to divulge information then you must expect to be punished accordingly.

(10) Everyone has the 'right to life' and it's about time we stepped up to the mark and begin to better protect that right.

Roger Bennett
October 2013

Written evidence submitted by Guardian Media Group [CT 17]

1. In late 2012 Edward Snowden was working as an analyst for Dell inside a US military base in Japan. In the three months before May 2013 Snowden had moved to work for the US government contractor, Booz Allen Hamilton, at a signals intelligence operations centre in Hawaii. The US signals intelligence service is known as the National Security Agency or "NSA". It operates under the jurisdiction of the US Defense Department.

2. Edward Snowden was one of a huge number of people with US Government clearance to access large quantities of electronic data about NSA surveillance activities as well as the activities of the UK's GCHQ.

3. Snowden gave documents to Glenn Greenwald, then a Guardian columnist based in Rio, in late May 2013. Snowden also gave material to Laura Poitras, and Academy Award-nominated independent filmmaker based in Berlin, who has specialised in intelligence matters, and Bart Gellman, a Pulitzer prize winning journalist at the Washington Post. The Guardian's veteran former diplomatic editor, Ewen Macaskill, met Snowden in Hong Kong along with Greenwald and Poitras.

4. Using less than 1% of the documents it was given by Snowden, the Guardian has published stories about the changing nature of intelligence and how technology is leading to routine mass collection and analysis of phone, email, social media and text message data. We have revealed the close relationship between intelligence services and technology or telecom companies and examined how, in the opinions of some, technologies have moved ahead of the law. And we have disclosed how the intelligence agencies have, some believe, worked to undermine the security standards upon which the internet, commerce, financial institutions and individuals rely.

5. The Guardian was not alone in publishing these stories. Many other publications across the world including the New York Times, the Washington Post, Le Monde, Der Spiegel, El Mundo, Globo, the Hindu, Suddeutsche Zeitung and El Pais have also published stories based on the Snowden material. In each case the relevant editor independently took the view that these were matters of considerable public importance.

6. These stories have prompted vigorous debate in parliaments across the world, led to calls for legal reform in the US and Europe, and a number of legal challenges. The President of the US, the German Chancellor and the UK Prime Minister have set up or encouraged reviews of intelligence

and/or oversight mechanisms. Numerous academics, business leaders and technology experts have testified as to the public importance of the issues raised. On November 26 The United Nations moved a step closer to calling for an end to excessive surveillance in a resolution that reaffirmed the "human right to privacy" and called for the UN's human rights commissioner to conduct an inquiry into the impact of mass digital snooping.

7. We now briefly outline the nine stories published by the Guardian since June that demonstrate the Guardian's contribution to this global debate.

Verizon - NSA collecting phone records of millions of Verizon customers daily

8. **On 6th June**, the Guardian published its first story as a result of having access to the files provided by Edward Snowden. That story, entitled "**Verizon - NSA collecting phone records of millions of Verizon customers daily**" outlined that the NSA has been collecting telephone records of US Verizon customers under a top secret court order issued in April 2013 for a three month period until 19 July 2013.

9. The order requires Verizon to give the NSA all call records in its systems daily (between the US and abroad and wholly within the US). These details include the numbers of both parties, location data, time, call duration, unique identifiers, originating and terminating call, telephone calling card numbers, trunk identifiers, International Mobile Subscriber number, and comprehensive communication routing information. The data can include cell site location data. The NSA Court order explicitly bars Verizon from disclosing to the public either the existence of the FBI's requests for its customers' records or the court order itself.

10. The coverage has prompted a significant number of cross party US Government reviews initiated from the President through to members in both Houses including: Fourth Amendment Restoration Act, Surveillance State Repeal Act and legislation to reform domestic surveillance laws. Documents released in November 2013 showed the NSA's searches of a database containing the phone records of nearly all Americans violated privacy protections for three years by failing to meet a court-ordered standard. The newly declassified documents showed the violations continued until a judge ordered an overhaul of the program in 2009. The revelations called into question the public statements of Top U.S. officials, including the NSA's Gen. Alexander, who have repeatedly reassured lawmakers that the phone-records programme was "well-overseen" and carefully executed under oversight from the secret national security court.

11. As a direct result of the revelations in this first story, On 22nd November 2013, the American Civil Liberties Union was in court in its case *ACLU v Clapper*[1] to argue that this mass data collection violates Americans' constitutional rights of privacy, free speech, and association, and that it goes far beyond what Section 215 of the Patriot Act envisaged. On 29th October, Republican Senator and author of the Patriot Act Jim Sensenbrenner wrote that *"whatever our differences may have been in the past, we strongly agree that the dragnet collection of millions of Americans' phone records every day — whether they have any connection at all to terrorism — goes far beyond what Congress envisioned or intended to authorize. More important, we agree it must stop."*[2]

NSA Prism program taps in to user data of Apple, Google and others & **GCHQ had been gathering intelligence from internet companies under the Prism program**

12. On 6th & 7th June, the Guardian published two stories: **"NSA Prism program taps in to user data of Apple, Google and others"**, and **"GCHQ had been gathering intelligence from internet companies under the Prism program.**" These stories examined how since 2007 the NSA has been running a programme called Prism which enables the NSA to have direct access to the servers of some of the largest technology firms in the world including Google, Apple and Facebook.

13. In doing so, the NSA is able to covertly acquire and store the search history, email content, file transfers and live chats of any users of those websites without the knowledge of users. The second story demonstrated GCHQ's close involvement in the NSA collection of data, outlining how GCHQ has been accessing the Prism programme since June 2010 to gather intelligence on UK citizens. This story raised significant questions about the legal framework under which GCHQ was accessing vast amounts of personal data about UK citizens.

14. On 7th June, as a result of the Guardian coverage, the Chairman of the Intelligence & Security Committee, Sir Malcolm Rifkind issued a statement saying that "*the ISC will be receiving a full report from GCHQ very shortly and will decide what further action needs to be taken as soon as it receives that information."*[3] In its subsequent report published on 17th July, the ISC stated that it was satisfied that the activities outlined by the Guardian *"conformed with GCHQ's statutory duties*", but went on to say it would consider further whether the *"current statutory framework governing access to private communications remains adequate."*[4] On 31st October 2013, in a

1 https://www.aclu.org/blog/national-security/finally-day-court-challenge-mass-surveillance

2 http://www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-98953.html

3 http://isc.independent.gov.uk/news-archive/7june2013

4 http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf

Westminster Hall debate on oversight of the intelligence services, ISC member George Howarth MP confirmed that the Committee was only made aware of the existence of the Tempora programme *after* they read the article in the Guardian.[5]

15. As a result of the Guardian's reporting on these stories, English PEN, Open Rights Group and Big Brother Watch are in the process of challenging the legality of PRISM and Tempora at the European Court of Human Rights[6]. Separately, the Government and telecoms companies face a separate legal challenge brought by Privacy International against the UK's Investigatory Powers Tribunal over Tempora. Liberty Human Rights has made official complaint to IPT and asked for an investigation into whether Prism and Tempora systems breached Article 8 of the Human Rights Act in relation to regulation of access to personal information.

16. On Monday 4th November, the Guardian published an interview with David Blunkett MP and former Home Secretary at the time that RIPA was passed in which he said *"In government you are pressed by the security agencies. They come to you with very good information and they say 'you need to do something'… I think RIPA needs trimming back. It is being used for things for which it was never intended."*[7]

17. The Guardian's reporting for these first two stories was widely commended. For instance, Strobe Talbott, President of the Brookings Institute in Washington and a former Ambassador at large for President Clinton, commented*: "The Guardian us emerging as global source of old-fashioned journalism via new media: e.g., breaking data mining story. Good on them, good for us"*. Former President Jimmy Carter said the revelations had been "helpful", adding "*I think that the secrecy that has been surrounding this invasion of privacy has been excessive, so I think that the bringing of it to the public notice has probably been, in the long term, beneficial."*[8]

GCHQ spied on foreign politicians at G20 summits

18. On 17th June 2013, the Guardian published a story entitled, **"GCHQ spied on foreign politicians at G20 summits",** which outlined how the UK Government led by Gordon Brown had worked through GCHQ to monitor the phones and emails from allies including Turkey and South Africa during the G20 meetings in London in 2009. The interception of data enabled 45 analysts to monitor activity

5 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm

6 https://www.privacynotprism.org.uk/

7 http://www.theguardian.com/world/2013/nov/04/david-blunkett-review-laws-security-services

8 http://www.theregister.co.uk/2013/07/18/carter_warns_america_no_democracy_prism/

in real time, providing UK Ministers with intelligence on the positions of delegations attending the G20 event.

19. While the G20 interception capability gave British Ministers and officials advance notice of what allies were **l**ikely to say at multilateral meetings, the value of the intelligence gathered was considered of limited advantage. As such, the Guardian story prompted questions about whether spending significant budget on such activity was necessary given the economic pressures on Government budgets, and the central focus on counter-terrorism. As a result of the coverage, the Governments of Turkey and South Africa issued denunciations of spying and demanded an apology. Turkey called spying "scandalous" and the South African government demanded a full investigation. In October – after further revelations about the US and UK spying on diplomats and politicians from countries which would in other respects be regarded as allies – President Obama ordered the National Security Agency to stop eavesdropping on the headquarters of the International Monetary Fund and World Bank. [9]

How the NSA is still harvesting your online data

20. On 27th June 2013, the Guardian published **"How the NSA is still harvesting your online data".** This story highlighted the disparity between public statements by the US President Barack Obama that practices put in place by President George W. Bush to intercept had ceased. The White House had claimed that "*the internet metadata collection program authorized by the FISA court was discontinued in 2011 for operational and resource reasons and has not been restarted*."[10] The story outlined that NSA metadata programs were ongoing after 2011, enabling the collection of one trillion records. The story highlighted the fact that a substantial portion of internet data collected by the NSA comes from allied governments, including from GCHQ[11].

NSA leaks US bugging European allies

21. On 30th June, the Guardian published "**NSA leaks US bugging European allies"** which outlined how US intelligence services have been spying on the EU mission in New York and its embassy in Washington through devices in mission fax machines, electronic bugs, collection of transmissions and copies of computer hard drives. The story outlined how the US intelligence community has targeted the embassies and missions of 38 allied nations.

9 http://www.reuters.com/article/2013/10/31/us-usa-security-imf-idUSBRE99U1EQ20131031

10 http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

11 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

22. This story demonstrates that the intelligence agencies are increasingly driven by economic considerations, alongside any considerations of counter terrorism or national security. The fact that the US is bugging its allies led to the Spanish and German Governments summoning their respective US ambassadors to discuss the details of the story. In November, the German Government summoned the UK ambassador to discuss the allegations.

Microsoft NSA collaboration over user data

23. On 12th July, the Guardian published **"Microsoft NSA collaboration over user data",** which outlined how the US technology firm Microsoft collaborated with US intelligence services to allow its users communications to be intercepted, including helping the NSA to deliberately circumvent the encryption protocols that millions of Outlook.com and Hotmail customers rely on to keep their data and communications private. Microsoft also enabled the NSA's Prism programme to have easy access to its cloud storage service which has more than 250 million users worldwide. The story also outlined the fact that 9 months after purchasing the online video calling application Skype (which has over 650 million registered users worldwide[12]) Microsoft had worked with the NSA to develop a new capability that had tripled the amount of Skype video calls being collected through the Prism programme.

24. As a result of reporting by the Guardian, on 18th July, a group of digital and tech businesses petitioned the US Government, urging greater transparency around national security-related requests. Several proposed Acts including the Government Surveillance Transparency Act, and the Surveillance Transparency Act followed. On 30th August, Microsoft and Google began litigation against the US Government, seeking permission to tell the public how much surveillance information they have handed to the U.S. government.

25. In a further Guardian article on 12th September, speaking at a conference in San Francisco, Mark Zuckerberg of Facebook said, *"The government response was, 'Oh don't worry, we're not spying on any Americans.' Oh, wonderful: that's really helpful to companies' trying to serve people around the world, and that's really going to inspire confidence in American internet companies".* In reference to the tech companies actions to drive more transparency around data requests, Zuckerberg said, *"We are not at the end of this. I wish that the government would be more proactive about communicating. We are not psyched that we had to sue in order to get this and we*

12 http://www.telecompaper.com/news/skype-grows-fy-revenues-20-reaches-663-mln-users--790254

take it very seriously". On being asked why the tech industry had not been clearer with consumers about what the US surveillance industry was up to, the CEO of Yahoo Marissa Mayer, said, *"Releasing classified information is treason and you are incarcerated*"[13].

26. The Guardian's publication of this story demonstrated the gap between the tech industry's outward-facing attitude to consumer privacy and its actual cooperation with Government to supply access to vast amounts of data generated by users. Without the Guardian's publication of this story, given the classified nature of the material, it is likely that the tech industry would have remained silent, and that millions of innocent consumers would have been unaware of the intelligence agencies' activities as a result.

27. In response to a further Washington Post story Microsoft's top lawyer called "disturbing" a new report saying the U.S. government may be eavesdropping on the company's Web traffic overseas. Brad Smith, Microsoft's general counsel said: *"If they are true these actions amount to hacking and seizure of private data and in our view are a breach of the protection guaranteed by the Fourth Amendment to the Constitution*". In common with other west coast tech companies – including Google and Yahoo – Microsoft moved to improve its encryption.[14]

NSA pays £100m in secret funding for GCHQ

28. On 1st August, the Guardian published **"NSA pays £100m in secret funding for GCHQ",** which outlined the fact that a weaker system of regulation governing the activities of the British intelligence agencies in relation to the collection and interrogation of data is being used as a 'a selling point' to the NSA who sub contract espionage activity to GCHQ for £100m paid over three years. Through this contract, GCHQ supplies the NSA with personal data gathered from the mobile phones and digital applications to enable it to "*exploit any phone, anywhere, any time*". As a result of this funding from the NSA, GCHQ is in a position where it must "*pull its weight and be seen to pull its weight"*[15].

29. While it has been known for many years that the UK and US intelligence communities have a close relationship, before the publication of the article by the Guardian GCHQ supports the NSA in this way, acting to explicit or perceived service level agreements regarding output delivery. It was also

13 http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

14 http://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story_1.html

15 http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

not known that the UK intelligence services explicitly use the weaker oversight regime in the UK as a key reason for conducting intelligence operations in Britain, saying *"we are less constrained by NSA's concerns about compliance."*[16]

Revealed: how US and UK spy agencies defeat internet privacy and security

30. On 6th September, the Guardian published "**Revealed: how US and UK spy agencies defeat internet privacy and security".** The article detailed a 10 year, $250m-a-year NSA program which works covertly with tech companies to insert weaknesses into products. *"For the past decade, NSA has lead [sic] an aggressive, multi-pronged effort to break widely used internet encryption technologies…Vast amounts of encrypted internet data which have up till now been discarded are now exploitable."*[17]

31. The document which sits at the heart of reporting the encryption story acknowledges the fact that there would likely be public interest if these revelations were ever revealed, stating that "*Some exploitable products are used by the general public; some exploitable weaknesses are well known eg possibility of recovering poorly chosen passwords…Knowledge that GCHQ exploits these products and the scale of our capability would raise public awareness generating unwelcome publicity for us and our political masters."*[18]

32. Both the UK Government through the Cabinet Office, and the heads of the UK intelligence services acknowledge the dangers of weaknesses in cyber security to the UK economy. A report published by the Cabinet Office undertaken by government technology supplier Detica, found that the cost of cyber crime to the UK economy is £27 billion per annum[19]. During the recent Intelligence and Security Committee open session with the intelligence chiefs, Director of GCHQ, Sir Iain Lobban, said that, "*We are seeing threats to over 20 industrial sectors. Research and innovation being targeted, trade secrets, academic research, as I said. Industrial espionage on an industrial scale, stealing intellectual property. The response to that has to be a cross-Government one and actually a beyond Government one. We work very closely with the Centre for the Protection of National Infrastructure. We work with the Business, Innovation and Skills department. We will be working increasingly with the new National Crime Agency, who work with the Cabinet Office, of course.*

16 http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

17 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

18 http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

19 https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report

That is a team game. If we get that right, I believe that we can actually be world class in terms of cyber, the UK."[20]

33. Responding to revelations that UK and US intelligence agencies have been weakening the fabric of the internet, an Economist editorial read, *"This is big news, if true… encryption of electronic data is an essential part of modern life. It secures the financial networks that link the world's banks, protects credit cards, stops mobile-phone calls from being listened to, guards medical records and lawyers' letters to their clients. Though cybercrime is a growing menace, reliable encryption remains the foundation on which the trillion-dollar edifice of e-commerce is built: without it, nobody would be able safely to make a payment online. For critics, sabotaging such codes is akin to a government secretly commanding lockmakers to make their products easier to pick—and to do so amid an epidemic of burglary."*[21] The British creator of the World Wide Web, Sir Tim Berners-Lee, told the Guardian that the "*agencies' decision to break the encryption software was appalling and foolish."*[22] An influential group of academic cryptographers wrote an open letter calling for the ISC to "*investigate as a matter of urgency".*[23]

34. Two leading US professors of computing wrote in Foreign Affairs, the journal of the US Council on Foreign Relations*: "Of all of the revelations about the NSA that have come to light in recent months, two stand out as the most worrisome and surprising to cybersecurity experts. The first is that the NSA has worked to weaken the international cryptographic standards that define how computers secure communications and data. The second is that the NSA has deliberately introduced backdoors into security-critical software and hardware. If the NSA has indeed engaged in such activities, it has risked the computer security of the United States (and the world) as much as any malicious attacks have to date. No one is surprised that the NSA breaks codes; the agency is famous for its cryptanalytic prowess. And, in general, the race between designers who try to build strong codes and cryptanalysts who try to break them ultimately benefits security. But surreptitiously implanting deliberate weaknesses or actively encouraging the public to use codes that have secretly been broken -- especially under the aegis of government authority -- is a dirty trick. It diminishes computer security for everyone and harms the United States' national cyberdefense interests in a number of ways."*[24]

20 http://isc.independent.gov.uk/files/20131107_ISC_uncorrected_transcript.pdf

21 http://www.economist.com/news/international/21586296-be-safe-internet-needs-reliable-encryption-standards-software-and

22 http://www.theguardian.com/world/2013/nov/06/tim-berners-lee-encryption-spy-agencies

23 http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html

24 http://www.foreignaffairs.com/articles/140214/nadia-heninger-and-j-alex-halderman/tales-from-the-crypto-community?cid=soc-twitter-in-snapshots-tales_From_the_crypto_community-103013

35. On reviewing the Home Affairs Select Committee's recent enquiry into e-crime, it appears that the Committee was not made aware of the intelligence agencies' remit in this area, nor its activities in working with the tech community to alter encryption standards[25]. In publishing this story on encryption, the Guardian has brought to public attention the fact that digital products and services used by consumers and businesses across the world are potentially more vulnerable to attack as a result of intervention by our own intelligence agencies.

NSA and GCHQ target Tor network that protects anonymity of web users

36. On 4th October, the Guardian published a story **"NSA and GCHQ target Tor network that protects anonymity of web users",** which outlined the fact that the NSA had been targeting the encryption tool – originally designed and released by the US Navy to aid secure transfer of communications and still largely funded by the US State Department – by identifying users and attacking vulnerable software on their computers. The Guardian article outlined a range of weaknesses that had historically been exploited by GCHQ and the NSA, all of which had been fixed voluntarily by the Tor community membership months before publication of the Guardian story.

37. Tor has been the subject of attack by a range of repressive regimes in recent years. According to a presentation by a Tor developer, the protocol has been under attack as a result of: DNS filtering of the Tor website in Thailand in 2006 and throttling of Tor traffic in Iran, Tunisia and China in 2009.[26] At the height of the Arab Spring, the Tor project estimates that between 200,000 to 500,000 activists used Tor to communicate across Tunisia, Egypt, Syria and Iran in order to protect their anonymity. It was this ability to communicate that inspired these societies to revolution and to communicate that revolution to the outside world.

38. The centrality of Tor to both freedom of expression and its use by criminal elements has been recognised by the Coalition Government. On 1st November 2011, the Foreign Secretary William Hague told a London conference on Cyberspace that, " *Cultural differences are not an excuse to water down human rights, nor can the exploitation of digital networks by criminals or terrorists be a justification for states to censor their citizens."*[27] More recently on 11th July 2013, 3 months before the Guardian published its story on Tor, the Prime Minister gave a speech at the NSPCC in which he said that in the law enforcement agency is already doing a good job in '*disrupting the so called hidden internet"* and that they would get more funding to *"shine a light on this hidden*

25 http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf

26 http://internet-science.eu/sites/internet-science.eu/files/RunaSandvikEINSsummerschool%5B1%5D_0.pdf

27 https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace

internet"[28]. Just after the Guardian published its story on 10th October 2013, the head of the National Crime Agency said, "*You may think that you can operate anonymously online and have the security of Tor to conduct your business but you can't"*[29].

39. The Guardian's story about the efforts of the NSA and GCHQ to exploit weaknesses in the Tor network related to historic - not live – events. The weaknesses detailed by the Guardian and patches designed to fix those weaknesses have been openly discussed in forums used by Tor users for many months before the story was published. The fact that UK law enforcement agencies are attacking hidden protocols such as Tor is, again, not news, having come from the Prime Minister's mouth and being covered by many newspapers on Fleet Street in July this year. However, as the Foreign Secretary said in 2011, the use of digital networks by terrorists and criminals should not be used as an excuse to close down debate about the activity of Government that potentially undermines freedom of expression online in the UK.

Guardian Media Group

27th November 2013

28 https://www.gov.uk/government/speeches/the-internet-and-pornography-prime-minister-calls-for-action

29 http://www.telegraph.co.uk/technology/internet-security/10369880/National-Crime-Agency-wages-war-on-Tor-darknet-anonymity.html

Written evidence submitted by Birnberg Peirce & Partners [CT 18]

Evidence on Counter Terrorism - re: oral evidence 12th November 2013 relating to Mohamed Ahmed Mohamed ('CC')

We regret that we did not have immediate sight of the transcript of the above evidence given to the Committee. We hope nevertheless as the issues are of continuing importance in public debate it may still be of assistance for us to provide clarification of a number of points on which the factual evidence presented to the Committee has, we believe, been incorrect or is deserving of further supporting material for a full explanation.

We represented Mr Mohamed as his solicitors following his arrival in the UK on 14 March 2011, after he had been removed against his will from Somaliland to the UK (as opposed to Somalia where he lived with his wife and child) and was upon arrival placed under a Control Order and required to live in Ipswich.

A number of legal challenges came to be made on Mr Mohamed's behalf. All of these have far wider significance than for his case alone.

The central issues on which the courts had to decide were:

1. The legality of the Control Order imposed on 'CC' at the airport when he arrived in the UK on 14 March 2011.
2. The subsequent legality of the TPIM (Control Orders having given way to TPIMs in January 2012). (The challenges to these two orders were conjoined in proceedings in the High Court.)
3. The lawfulness of the Schedule 7 examination of CC at Heathrow Airport.
4. The evidence that supported an allegation of "tampering" with the G4S/GPS tag worn by him between 19th April and 16th May 2013.
5. The sequence of the allegations of breaches of the Control Order and the TPIM and their treatment by the courts.

We start with the period of time in which Mr Mohamed was imprisoned for breaches of obligations placed upon him by first the Control Order and then the TPIM.

<u>The sequence of the allegations of breaches of the Control Order and the TPIM and their treatment by the courts.</u>

Mr Mohamed was arrested, as the evidence given to your Committee by Charles Farr correctly stated, for breaches of the Control Order between August and October 2011. (Thereafter he was charged with breaches of the TPIM.) The evidence on this issue given to the Committee, came in answer to questions from Michael Ellis MP:

> Q. "Despite 14 allegations of a breach of a Control Order and 6 allegations of a breach of TPIMs, he keeps on being re-admitted to bail from custody by the courts ... ?" [Further evidence related to a third accusation, concerning alleged tamper with his tag in relation to which he was released in August 2013. We comment on this separately.]
>
> Q. "If cases of these breaches had not been stayed (pending the High Court's consideration of the legality of the Control Order and TPIM), would he have been in prison?" "Almost certainly serving a sentence of more than a year in prison?"

A. (Charles Farr) "That is correct.

Q. "He played the legal system?"

A. "I can't comment on that".

Q. "No I can".

The comments we would make are these;

a) Mr Mohamed, remanded in custody for the 14 and 6 breaches, had at the time of his respective releases on bail, already served over 8 months on remand in prison. It had already been acknowledged by the prosecution by the time of his release on 6th August 2013 for the third "tamper" allegation, that even if he had been convicted of the previous breaches at a subsequent trial, he would have already served more than his sentence for those breaches by reason of the time he had already spent in prison.

b) The context of the 14 and 6 breaches was this; Mr Mohamed had been seized in what later emerged as a joint "operation" with UK agencies by forces in Somaliland. The description he subsequently gave was of severe ill treatment for two months by Somaliland officers including treatment categorised as constituting torture for two months – the questions put to him while detained focussed on information relevant to the UK. At the conclusion of his detention in Somaliland, instead of being returned as he had asked to Somalia where he had resided for many years with his wife and child, he was forcibly removed to the UK. Immediately on arrival he was placed under a Control Order and required to live in Ipswich where he knew nobody. He was not only traumatised from his experience beginning on 14th January 2011 (of which medical evidence was available to the courts) but was entirely isolated in Ipswich. For that reason and others, a number of the severe regulations upon him, imposed by the Control Order were breached by him. At the time of his arrest, for a second set of breaches, he commented that he preferred to be in prison, as at least he would be with other people.

c) We feel it necessary to bring to your attention two earlier and not dissimilar cases of breach of Control Orders, both cases involving absconsion (of Ceri Bullivant and 'AN') which ended in both cases with their acquittal - in the case of Ceri Bullivant by a jury who accepted that he had reasonable excuse because of his despair at the crushing of any normality of existence for him (the Control Order was subsequently revoked by the High Court in any event). Mr Bullivant had absconded from the address at which he was required to live, but subsequently returned and handed himself in to the police, was arrested, charged and tried. In the second case 'AN', a Londoner, who was a victim of torture when a student in Syria, was placed on his return to the UK under a Control Order in Leicester (into a similarly isolated existence). He also absconded, was arrested, and spent a lengthy time on remand in Belmarsh prison. The criminal prosecution against him for breach was ultimately dropped and he was formally acquitted when the Control Order was quashed (following a decision in the House of Lords and subsequent decision by the High Court that the Control Order was void *ab initio*).

The evidence that supported an allegation of "tampering" with the G4S/GPS tag worn by him between 19th April 2013 until 16th May 2013.

d) The third allegation against Mr Mohamed, made on 25th July 2013, was as Mr Farr correctly stated in evidence based on claims by G4S that he had "tampered" with a GPS tag (on the 16th May 2013). The circumstances of his being granted bail on that allegation (almost immediately) deserve separate attention.

e) By the date that he was charged with the alleged tag tamper (as we set out above) he had served any potential sentence for the outstanding breach allegations. Moreover when Mr Mohamed was charged with this offence, there were separately before the Central Criminal Court identical allegations made by G4S in relation to two other unconnected TPIM wearers of GPS tags, 'TP' and 'CE'. All were granted bail by very experienced Old Bailey judges on the basis that the growing statistical improbability of tampering by a significant number of TPIM subjects all wearers of the GPS tag was exceptional.

f) On 22nd October 2013 the prosecution communicated formally with this firm that it would no longer pursue this tampering case against Mr Mohamed. Simultaneously the prosecution communicated the same decision in relation to the other two cases ('CE' and 'TP'). Police at the same time indicated to a fourth individual under a TPIM, bailed to return to the police station on the same allegation, that no further action was to be taken in relation to him. A similar approach, to our knowledge, is currently being taken in relation to other cases where the tags are cracking or malfunctioning in very similar ways. This extraordinary situation has we believe been brought about by the following accidental sequence of events.

(i) By accident of historical representation, this firm was already representing a number of individuals on TPIMs who were wearing the new (introduced in or around April 2012) GPS satellite tag. A growing number of arrests took place of separate individuals, not known to each other all of whom expressed astonishment at the allegation by the monitoring company G4S, that they had deliberately interfered with their tags. (Solicitors representing a further individual reported that a similar allegation had been made in his case.)Two reports of "tampering" for two separate individuals came when they had on separate occasions, in separate cities, been praying in a mosque.

(ii) Over a period of a year, this firm had already expressed clearly in writing to the police and the Crown Prosecution Service our belief that there was a malfunction of the tags, and that individuals were being arrested and prosecuted when the failure emanated instead from G4S's faulty equipment and/or inadequate research. In this regard we attach a note for your consideration summarising the position of the evidence within CC's prosecution and others for the same offence.

(iii) The Committee's attention is drawn to the opinion of Ross Anderson of Cambridge University (Professor of Security Engineering at Cambridge University) who raised a very real concern that the damage to the tag could be caused by recurrent stress fractures (of the kind that for example caused Comet aircraft to be grounded in the past). It appeared to the independent experts consulted by the defence that G4S had placed the large GPS tag introduced in April 2012 on the same strap tested for use only on the much smaller previous tag, with additional strain inevitable. It should be noted that no testing, despite repeated requests that this issue be considered, to our knowledge, was done of a further likely cause of strain inevitably caused by praying five times a day. Requests by defence experts to conduct tests and to

have access to test results to establish (or refute) these clearly stated propositions had not been met when the cases were all suddenly discontinued by the CPS.

g) On 1st November 2013 this prosecution against Mr Mohamed was formally discontinued (the prosecution against TP and CE had been discontinued at an earlier hearing on 30th October 2013). We requested from the Prosecution both in writing and orally at the Court the forensic reasons behind the prosecution's decision to discontinue the cases. The Court had expressed itself as sympathetic to the defence request, but as yet the prosecution have provided only a general answer that there was "insufficient evidence to proceed". The same explanation was given by the Home Secretary in her reply to your raising of the same question in the debate on 4th November 2013;

"*I urge her to look at the role of the G4S and the tags that have been provided*".

The adequacy of the Secretary of State's answer is one with which we are bound to take issue;

"*the police believe that in this case the tag functioned exactly as it should have done ..... he referred to the court case. The issue was not about the effectiveness of the tags, but about weakening the evidence threshold for taking a criminal prosecution in relation to the operation of the tags*".

h) No answer given to date has provided any satisfactory explanation as to how three entirely separate individuals came to be arrested and prosecuted on the basis of claimed "scientific evidence" and how it was that all three prosecutions came to be discontinued following a direct challenge in advance of any trial by the defence to the reliability of the G4S tags.

i) Our concern regarding the issue of tags remains, following the evidence of David Anderson QC at your Committee's hearing on 12th November 2013. The impression may have been left that no one now accused of tampering with their tag can be prosecuted. This is very far from the case. There have been many prosecutions in the past and no doubt ongoing for tampering allegations relating to the smaller tag. No doubt also there can and will be in the future prosecutions for damage or interference with the larger GPS tags. What is the issue here in these particular cases is very specific, that without evidence that the individuals had actually tried to remove their tags evidence of strain on the tag strap was repeatedly interpreted as deliberate "tampering". The claimed scientific opinion on which each prosecution relied can be summarised thus: that there was no innocent explanation for the strain.

j) We note that the Committee received private evidence from G4S about the tags. We do not know the reasons for this. Clearly we have a concern that at present no one, including the Committee knows why Mr Mohamed's case, and others, were discontinued. This is not intended to constitute an abstract quest for information. Not only did the individuals in question spend time in prison before bail (unusually) was granted by judges at the Old Bailey in each case, on the basis of these allegations, but the G4S GPS tags are still being used. The question relates of course furthermore to matters concerning the public purse. (In the accompanying note we refer to the report by NAPO of June 2012, identifying concern as to "technical failures" of electronic tags generally, not limited to the larger GPS model.)

k) We would welcome making available any further material that might assist to the Committee should it wish to conduct further examination of this issue.

The lawfulness of the Schedule 7 stop.

On his arrival at Heathrow airport on 14 March 2011 Mr Mohamed was detained and questioned for 6 hours under Schedule 7 of the Terrorism Act. Approximately 118 questions were prepared and submitted by the Security Service to the Counterterrorism Unit of the Metropolitan Police Service for this examination. Furthermore before the Schedule 7 interview the interviewing officers were instructed by email in the following terms:

"*We would be grateful if you would NOT be drawn into any discussion with MOHAMED regarding HMG [Her Majesty's Government] involvement in his arrest. You should be aware that any such write up is likely to be disclosable in any future civil proceedings.*"

The above evidence was given in the court proceedings that followed the imposition of a control order on Mr Mohamed at Heathrow airport. In separate judicial review proceedings brought on behalf of Mr Mohamed to examine the legality of the stop, Collins J found his detention and questioning under Schedule 7 to be unlawful. The questioning was not being conducted for the purpose of the Act, namely to establish whether or not he was involved in acts of terrorism, as the SSHD already was claiming he was, and had made a Control Order on that basis even before he had been detained in Somaliland (explained below)). Instead it was argued, the stop was being conducted for an unlawful purpose, of getting information from Mr Mohamed that was not tainted by torture in Somaliland. We provide the decision of Mr Justice Collins dated 20 December 2011. This judgment is of importance, beyond Mr Mohamed's case, defining the breadth of Schedule 7 powers. The fact of the Schedule 7 stop links with the further issue canvassed below as to the British authorities' knowledge of Mr Mohamed's detention in Somaliland and his treatment there, and in turn to the wider issue of the UK's alleged complicity in unlawful acts outside the UK.

The Legality of the Control Order/TPIM

The legality of the Control Order/TPIM itself was in question throughout after Mr Mohamed was notified of its existence at Heathrow Airport on 14th March 2011. That issue is at present listed to be considered by the Court of Appeal on 23rd January 2014. The appeal, due to be heard together with a second linked case CF, will consider very serious allegations regarding the potential complicity of the UK Government (and its agents) in unlawful acts including the arrest, detention, torture in Somaliland and subsequent unlawful deportation of both CC and CF. It has been argued, that but for the unlawful actions of the UK, Mr Mohamed would not have been within the jurisdiction to be the subject of a Control Order.

We are aware that you already identified the fundamental question; i.e. why was Mr Mohamed in the UK at all? He at no time, we confirm, wished to be. We observe that the Committee was not provided with a considerable amount of evidence available to the Home Office, on the record within previous court hearings, that could have provided the answer to your question.

The sequence of the events leading up to Mr Mohamed's arrival in the UK on 14 March 2011 was as follows:

Up until his arrival Mr Mohamed had lived in Somalia since 2007, with his wife with whom he had a child. His wife was pregnant with their second child. Mr Mohamed had no intention of returning to the UK. Nevertheless on 13th January 2011, whilst he was outside of the jurisdiction in Somaliland, the Secretary of State for the Home Department sought and was granted permission from the High Court to make a non-derogating Control Order, i.e. a UK executive measure that can be applied only to persons who are within the UK. On 14th January 2011, the day after the Control Order was made, Mr Mohamed was arrested and detained in Somaliland in what was described by the local media as a "*Joint security operation of Somaliland and British intelligence*". Mr Mohamed subsequently reported that during the two months of his detention in Somaliland that followed he had been tortured and subjected to inhumane treatment without any recourse to legal due process. On 13th March 2011, he was removed from Somaliland, despite requesting that he be returned to Somalia to his wife and child, on a one-way travel document provided by British officials in the British Embassy in Addis Ababa. On his arrival at Heathrow airport, he was detained and questioned unlawfully, as the High Court held, under Schedule 7 TA 2000. The questions mirrored those asked when he was interrogated in Somaliland, including under torture.

Serious questions concerning the UK's complicity in Mr Mohamed's treatment in Somaliland were directly raised within Mr Mohamed's Control Order/TPIM challenge. Whilst part of the proceedings were conducted in secret session, nevertheless evidence was disclosed in open session that supported Mr Mohamed's contentions (and those of "CF"). That open evidence we suggest must cast considerable doubt on the evidence given to the Committee on 12th November 2013 in which the Home Office witness Mr Farr stated (in response to your question as to why Mr Mohamed was in the UK) that the British Government had, "*an obligation .... to arrange his removal back to the UK*".

The full background necessarily underscores very serious questions; the degree of knowledge and involvement of the British authorities in Mr Mohamed's arrest, treatment and forcible return back to this country, with the intention of placing him on a Control Order (at cost not only to him but to the public purse), that Control Order having been made some two months before his arrival on UK soil. The impression the Committee may have at present is that Somaliland had instigated the request for his return to the UK after lawful detention there, and on their own volition, without the involvement of the UK hitherto.

We hope that this letter may serve to demonstrate the complex and serious issues that were raised during the passage of the cases concerning Mr Mohamed.

Encl:
1) Explanatory note re G4S GPS tag cases
2) Judgment of Collins J, CC v CPM and SSHD [2011] EWHC 3316 (Admin)
3) Guardian article (Ian Cobain, *The real question about the terror suspect who fled in a burqa: did M/5 bring him here illegally?* 14/11/2013). We include this as the only press report to date which has conducted an investigation of the underlying evidence.

Birnberg Peirce & Partners

29 November 2013

NOTE ON G4S GPS TAGS

Re: Cases of breach of TPIM discontinued by the CPS.

On the 1st November at the Central Criminal Court case alleging breach of a TPIM was discontinued by the Crown Prosecution Service. It was the third such case that week on which the Crown offered no evidence. All three cases concerned allegations of tampering with GPS tags and the circumstances of their discontinuance can only raise serious questions as to the reliability of the G4S made GPS tag.

This firm has represented two thirds of those currently on TPIMS in the country (6 out of 9) – and all of those we represent have been accused of the criminal offence of tampering with their GPS tags, an accusation which all strenuously denied from the outset in police interview and in subsequent correspondence from their lawyers to the CPS. A fourth case was also, discontinued in early November, after an earlier arrest, confirming, it would appear, that neither the police nor the CPS feel confident in the expert evidence on which prosecutions had been mounted which had asserted intentional tampering. Although the allegation has been made against all six individuals by G4S, some instances were not prosecuted. Since the three prosecutions were discontinued in early November, a number of other apparently identical incidents have arisen and are still arising.

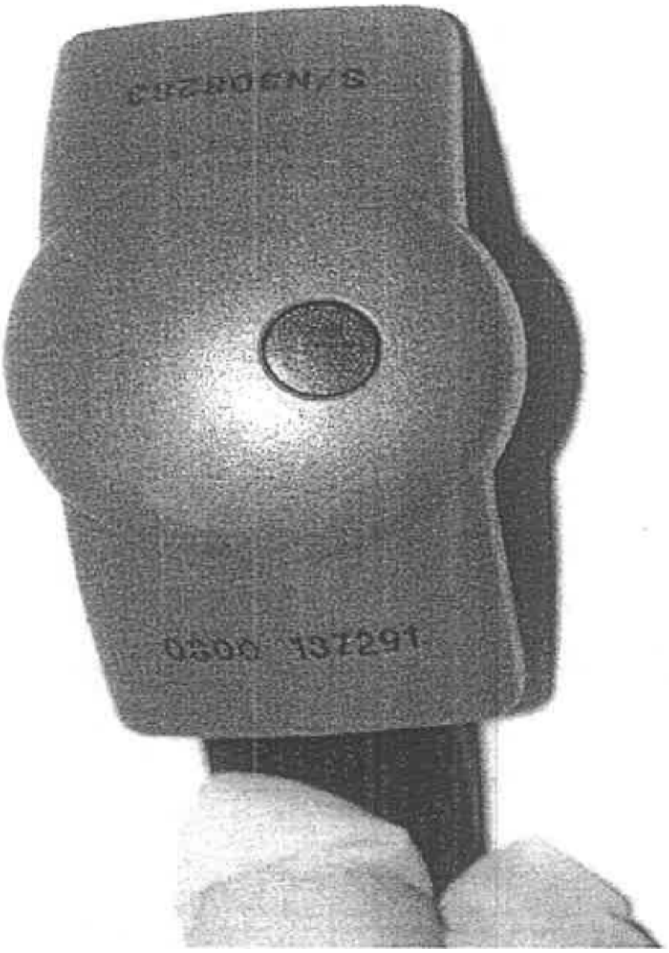
History of the GPS Tag

G4S promote their tags on their website thus:
"The technology associated with tagging has been proven to be robust and reliable. It has been thoroughly tested and the equipment is constantly updated to take advantage of the latest technology as well as ensuring it remains tamperproof…

An active programme of new product development ensures that both our support technology and monitoring equipment is state-of-the-art".

The GPS tag was introduced for those on TPIMS, along with other cases, in April 2012. The GPS model is considerably bulkier than its predecessor – as these images show.

Original Tag



GPS Tag

We know from its website that G4S placed the much bulkier unit of the GPS tag on the same strap that is used for the previous smaller tag http://www.g4s.uk.com/en-GB/What%20we%20do/Services/Care%20and%20justice%20services/Monitoring%20Technologies/OM247-SOLO%20GPS%20Tag/ (see attached).

Two experts instructed by the defence, made the following comments on the three recent cases.

Ross Anderson FRS FREng, Professor of Security Engineering at Cambridge, said:

"These are just the latest cases in a whole series. Britain's current curfew tagging systems are not fit for purpose. Systems can provide high levels of false alarms, and operators have difficulty telling false alarms from real ones.

The quality of evidence is poor, and in at least five cases now, when defence experts have asked to examine the tags a defendant was supposed to have tampered with, or the systems, or even samples of straps and clips, the prosecution has been withdrawn or collapsed.

In the case of these defendants, the curfew contractor appears to have fitted large, heavy GPS curfew tags using straps and clips that were tested and approved for use with the much lighter curfew tags fitted to people serving short community sentences. It is not at all surprising that the clips eventually fractured.

Every engineering student learns how fatigue fractures caused two Comet airliners to crash. It is strange that these were not even considered. It is also strange that the Ministry of Justice did not have tags tested for the strain imposed by people praying five times a day. The defendants appear to have been wrongly prosecuted as a result of official incompetence"

Dr. David Schudel, Keith Borer Consultants said,

"One of the striking things about the new GPS units is their size compared to the old PID "tags". The new GPS devices are bulkier and protrude from the leg lending themselves open to being snagged, twisted or rotated away from the leg, and are generally likely to be subject to greater forces in normal wear than the old style tags. Yet despite the significant change in size, it appears the same attachment clips and straps have been used as before. There seems to be a high rate of failure of these new GPS devices which manifests as a tamper-alert but with the device still fixed to the leg".

The CPS discontinued these cases after the defence had requested basic data regarding the integrity of the tags, including confirmation of the testing that had been carried out on the new GPS tag. This led to the prosecution first requesting an adjournment of the Pleas and Case Management hearing and subsequently offering no evidence. Following notification of discontinuance of the cases this firm wrote to the

CPS requesting confirmation of the forensic basis for discontinuance of the cases but to date the CPS has informed us only that they considered there was insufficient evidence to proceed.

Background to the Electronic Tagging Cases (GPS)

The Home Office, in relation to the cases of individuals who are the subject of the successor to Control Orders (TPIMs) required that each individual wear an electronic tag (a device that registers to a central monitoring company when the individual leaves and arrives at the address in which he is authorised to live). Until 2012 individuals subject to such a regime (just as many individuals on bail facing criminal charges and subject to conditions), were required to wear a standard electronic tagging device. After 2012, the individuals under TPIMs were required to wear the larger device (GPS) which claims the further capacity to register their whereabouts.

The company contracted with the Home Office/Ministry of Justice to provide the devices is G4S (and in some areas of the country SERCO). For more than a year and a half, after each allegation of tamper with the larger GPS tag came to be made against first one then another and then ultimately all of the individuals we represent subject to TPIMs, all strenuously denied that they deliberately, or even consciously, interfered or tampered with their tags.

TPIMs are civil orders by the Executive which impose restrictions such as who the individual can meet, where the individual can go and what in practical terms the individual is able to do. However to breach any of those restrictions, including to tamper with the tag, constitutes a criminal offence for which the individual concerned is liable to a sentence of up to five years' imprisonment. The individual faces a trial before a jury, which will be told that he is in breach of an obligation imposed under the TPIM regime (and that the breach of the obligation is an offence under the Terrorism Act). What the jury will not be told (and what the individual himself will never have been told, in any or any adequate detail) is why he is under that regime – that much is produced in secret evidence only.

The principle upon which electronic tagging systems are based is of a rubber strap which clips inside the device. If the strap is broken, an optic question mark is exposed, and sets off a "tampering" alarm.

The company concerned has claimed that extensive testing was carried out to establish the tag's reliability and, if any, vulnerabilities. Experts relied upon by the prosecution have produced reports which assert its reliability. No tests appear however, ever to have been done on the strap once the far larger electronic monitoring device (the GPS) came to be attached yet the strap is identical to that used for the smaller device. What it appears was never factored in, is the additional degree of strain that the larger device must place upon the strap, nor upon the clumsiness of the device and the far greater propensity to it being knocked and hit (more than one wearer of the new tag has reported tripping/falling down stairs, and knocking, for instance on a bicycle). A further factor for which confirmation of testing was very specifically requested was an assessment of the potential strain caused by praying five times each day. Our own lay observations of a demonstration of this aspect on several of the individuals concerned suggest it is also a factor deserving of further investigation. (Of the nine individuals subject to TPIMs (and the larger tag) eight had previously been subject to Control Orders (and the smaller tag) for a number of years and no allegations of tampering had been made against any during the Control Order regime.)

History of problems with the tags

Issues with the tags used by G4S have been raised previously. If, as it appears, there are particular issues concerning the design of the GPS tag – it would be a matter of considerable concern if these have not been bought to the attention of the Minister of Justice and the Home Secretary.

In June 2012 NAPO published a briefing *"Electronic Tagging – A Flawed System"* which cited 120 case studies and identified from them that an area of concern was *'technical failure'* (http://www.napo.org.uk/about/news/news.cfm/newsid/200). The Home Secretary responded that she would *'look very seriously at the report'* and was committed to ensuring the system was *'working properly'* http://www.bbc.co.uk/news/uk-18432500 .

The Minister of Justice asked in the Serious Fraud Office in July 2013 to investigate G4S for overcharging tens of millions of pounds on electronic tagging contracts for offenders http://www.theguardian.com/business/2013/jul/11/g4s-investigated-overcharging-millions-pounds. In the same month a G4S whistleblower made

allegations that the equipment was faulty http://www.dailymail.co.uk/news/article-2362785/G4S-whistleblower-Nigel-Mills-reveals-criminals-roaming-free-security-firm-blunders.html .

The future

These cases raise questions as to the tags' continuing use. If there is now compelling evidence to suggest they are unreliable, it is in the public interest that this be investigated. In particular any criminal prosecution must be mounted on the basis of sound evidence. Prosecutions based upon scientific evidence are governed by clearly established principles; that the evidence should be sound, of the highest integrity, subject to rigorous safeguards and with the underlying data on which claims are made, open to responsible scrutiny by scientific peers. It is clearly entirely unsatisfactory that all that is presently known is that these cases were discontinued, initiated as they had been by claimed expert assessments in each case that there was no innocent explanation for the tamper.

Birnberg Peirce and Partners
29th November 2013

Case No: CO/5457/2011

Neutral Citation Number: [2011] EWHC 3316 (Admin)
IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION
ADMINISTRATIVE COURT

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 20 December 2011

Before:

MR JUSTICE COLLINS

- -

Between :

CC	Claimant
- and -	
The Commissioner of Police of the Metropolis	1st Defendant
- and -	
Secretary of State for the Home Department	2nd Defendant

- -
- -

Mr Tim Otty Q.C. & Mr Dan Squires (instructed by **Birnberg Peirce**) for the Claimant
Dr Dijen Basu (instructed by **Solicitors to the Metropolitan Police**) for the 1st Defendant
Mr Jonathan Hall (instructed by **The Treasury Solicitor)** for the 2nd Defendant

Hearing dates: 5 December 2011

- -

Judgment

Mr Justice Collins:

1. The claimant has anonymity because he is subject to a control order imposed under Section 2 of the Prevention of Terrorism Act 2005 and it has been decided that he should have anonymity in connection with that order. That anonymity has been properly extended to this claim. In it the claimant challenges the exercise against him by police officers at Heathrow Airport of powers to question and detain passengers arriving in, leaving or transiting this country to determine whether they appear to be terrorists within the meaning of the Terrorism Act 2000. The powers in question are conferred by Schedule 7 to the 2000 Act.

2. In the claim form and in his skeleton argument Mr Otty, Q.C. made wide ranging general submissions which sought to limit the circumstances in which the powers could be exercised. It is most important that the scope and extent of the powers as laid down in Schedule 7 should be determined and I have heard argument from all parties on that issue. All counsel accepted that the powers could not be used if the predominant purpose was other than that specified in the Schedule. In the end there was little between them since Mr Otty was persuaded that the extensive limitations on the powers for which he was contending in his written submissions were not appropriate. But it was and remained his case that on the facts the powers were not exercisable and so the detention and questioning of the claimant was not lawful.

3. I should first set out the relevant provisions of the 2000 Act. Section 1 defines terrorism in very wide terms. It provides as follows:-

> "(1) In this Act "terrorism" means the use or threat of action where –
>
> (a) the action falls within Subsection (2)
>
> (b) the use or threat is designed to influence the government or an international government organisation or to intimidate the public or a section of the public, and
>
> (c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.
>
> (2) Action falls within this subsection if it –
>
> (a) involves serious violence against a person,
>
> (b) involves serious damage to property.
>
> (c) endangers a person's life, other than that of the person committing the action,
>
> (d) creates a serious risk to the health or safety of the public or a section of the public, or
>
> (e) is designed seriously to interfere with or seriously to disrupt an electronic system …

(4) In this section –

(a) "action" includes action against the United Kingdom,

(b) a reference to any person or to property is a reference to any person, or to property wherever situated,

(c) a reference to the public includes a reference to the public of a country other than the United Kingdom

(d) "the government" means the government of the United Kingdom, of a part of the United Kingdom or of a country other than the United Kingdom …"

4. Thus terrorism for the purposes of the Act includes action which falls within the definition in subsections (1) and (2) in any country in the world and which may be aimed at the government of that country whether or not it is likely to affect the United Kingdom.

5. Section 40 of the Act gives an even wider definition of 'terrorist'. By section 40(1) a terrorist means a person who has committed various offences created by the Act and in addition by s.40(1)(b) who "is or has been concerned in the commission, preparation or instigation of acts of terrorism". S.40 (2) provides:-

> "The reference in subsection (1) to a person who has been concerned in the commission, preparation or instigation of acts of terrorism includes a reference to a person who has been, whether before or after the passing of this Act, concerned in the commission, preparation or instigation of acts of terrorism within the meaning given by section 1."

Thus once a terrorist always a terrorist whether or not the person in question has renounced his past or circumstances have changed (for example where the acts of terrorism occurred in a country whose government, perhaps because dictatorial and oppressive, has since been overthrown). Indeed, the terrorist may have become a respected and respectable member or even leader of the new government of that country. Nevertheless, he is still a terrorist within the meaning of the 2000 Act. I should make clear that when I use the word 'terrorist' I am applying the meaning set out in section 40 unless the contrary is stated.

6. Section 41 empowers a constable to arrest without a warrant any person whom he reasonably suspects to be a terrorist. Section 43 provides that a constable may stop and search a person whom he reasonably suspects to be a terrorist to discover whether he has in his possession anything which may constitute evidence that he is a terrorist.

7. Schedule 7, which is applied by section 53 of the Act, is headed "PORT AND BORDER CONTROLS". So far as material for the purposes of this case, it provides as follows:-

> "1.(1) in this schedule "examining officer" means any of the following –

(a) a constable,

(b) an immigration officer,

(c) a customs officer who is designated for the purpose of this schedule by the Secretary of State and the Commissioners of Customs and Excise …

2.(1) An examining officer may question a person to whom this paragraph applies for the purpose of determining whether he appears to be a person falling within section 40(1)(b).

(2) This paragraph applies to a person if –

(a) he is at a port …, and

(b) the examining officer believes that the person's presence at the port … is connected with his entering or leaving Great Britain … or his travelling by air within Great Britain …

(4) An examining officer may exercise his powers under this paragraph whether or not he has grounds for suspecting that a person falls within section 40(1)(b). "

Paragraph 5 provides that a person who is questioned pursuant to the powers contained in paragraph 2 must give any information and produce any documents in his possession which the officer requests. Paragraph 6 gives power to detain a person for the purposes of exercising the powers conferred by Paragraph 2, but only for a maximum period of 9 hours. Paragraph 8 confers powers to search a person or his possessions. Paragraph 18 provides –

"(1) A person commits an offence if he –

(a) wilfully fails to comply with a duty imposed under or by virtue of this Schedule …

(c) wilfully obstructs, or seeks to frustrate, a search or examination under or by virtue of this schedule.

(2) A person guilty of an offence under this paragraph shall be liable on summary conviction to

(a) imprisonment for a term not exceeding 3 months,

(b) a fine not exceeding level 4 on the standard scale, or

(c) both."

8. There is under the Schedule an obligation to answer questions put and to co-operate in any search. Failure to comply is a criminal offence and, if the failure was deliberate, the offence is committed. There is no defence of reasonable excuse. The powers created by Schedule 7 are far reaching and, so far as the power to detain is concerned,

affect the liberty of the person. Thus they must in principle be strictly construed and it is incumbent on the officer to inform the person that he is being detained and why. So much is established by various authorities, in particular *Pedro v Diss* [1981] 2 All ER 59, which concerned a power to detain conferred by section 66 of the Metropolitan Police Act 1839.

9. Schedule 8 of the Act deals with the treatment of persons detained under Schedule 7. Paragraph 1 enables the Secretary of State to designate places at which a person may be detained and any place so designated is to be regarded as a police station. The room in which the claimant was detained and questioned at Heathrow was not designated under Paragraph 1 and so was not a police station within the meaning of Schedule 8. Paragraph 6 provides:-

> "(1) Subject to paragraph 8, a person detained under Schedule 7 … at a police station … shall be entitled, if he so requests, to have one named person informed as soon as reasonably practicable that he is being detained there."

Paragraph 7 provides:-

> "(1) Subject to paragraphs 8 and 9, a person detained under Schedule 7 … at a police station … shall be entitled, if he so requests, to consult a solicitor as soon as reasonably practicable, privately and at any time."

Paragraph 8 confers powers on an officer of at least the rank of Superintendent to authorise a delay in compliance with requests made under paragraphs 6 or 7. Paragraph 9 enables an officer of at least the rank of Commander or Assistant Chief Constable to direct that the person detained can only consult a solicitor in the sight and hearing of a uniformed officer of at least the rank of inspector who has no connection with the detained person's case. I need not set out the grounds which can found action under Paragraph 8 or 9. There are also set out powers to take fingerprints and intimate or non-intimate samples and the circumstances under which those powers can be exercised are specified. Again, I need not for the purposes of this judgment set them out.

10. I should finally refer to Schedule 14 which deals inter alia with the exercise of his powers by an examining officer within the meaning of Schedule 7. Paragraph 4 provides:-

> "(1) Information acquired by an officer may be supplied –
>
> (a) to the Secretary of State for use in relation to immigration;
>
> (b) to the Commissioners of Customs and Excise or a customs officer;
>
> (c) to a constable;
>
> (d) to the serious Organised Crime Agency;

(e) to a person specified by order of the Secretary of State for use of a kind specified in the order …"

No relevant order has been made under paragraph 4(1)(e).

Paragraph 5 requires an officer to perform his functions in accordance with any relevant code of practice which the Secretary of State must make as laid down in Paragraph 6. I shall refer to the relevant provisions of the Code in due course. As will become apparent, in certain respects the Code in force at the material time which was issued in July 2009 is not entirely satisfactory.

11. Equivalent provisions to those contained in Schedule 7 have existed for some time, initially to help to combat terrorism from Ireland. Their primary purpose was and still is, as Lord Lloyd stated in his 1996 report (Cm 3420), 'to deter terrorists from entering the United Kingdom and to catch those who try; and to collect intelligence on the movements of persons of interest to the police and the Security Service.' In his annual report as the Independent Reviewer of the 2000 Act, Lord Carlile of Berriew, Q.C. has observed and considered the exercise of Schedule 7 powers and their value in combating terrorism. I quote from his 2004 report, which was one before me, but I have no reason to believe that what he says there has needed any modification since 2004. in Paragraphs 115 – 116 he says:-

> "115. Many examinations at ports are carried out after officers have received general or specific intelligence about a suspect, type of traveller, or characteristics of a suspected operation. Some are carried out as part of the work of gathering knowledge about individuals who have come to notice. Having watched the process, I am in no doubt that the trained and ingrained instinct of experienced officers still has real value … most stops are of perfectly decent and innocent travellers … [I]ntuition … is not the same as reasonable suspicion: much intuition cannot be rationalised. The continuation of the present system is a necessity in current circumstances, and can give rise to useful results, including intelligence gains, from time to time.
>
> 116. … The terrorist traveller has much to fear at UK ports of entry. It is likely that United Kingdom intelligence procedures and ways of sharing information to meet need are as good as anywhere. They are methodical and tireless. One of the consequences is that intuitive stops are likely to play a diminishing role – though one must be ever mindful of their utility, given the use of terrorist organisations whenever possible of 'clean skins, people with no past record of operational terrorist activity. "

12. The evidence before me shows that 97% of all examinations last less than 1 hour. Only 0.05% last more than 6 hours. Thus in the vast majority of cases detention is not required and does not occur. Neither the Schedule nor the Code indicate with any degree of precision the circumstances in which detention will occur. If the officers

decide to detain, the person concerned must be informed that he is being detained and why. This is done by means of a form TACT2. The Code states:-

> "Examination and detention under Schedule 7 are not the same. A person being examined will not necessarily need to be detained and it is envisaged that most examinations will be conducted without the need to detain the person. Detention will be required usually where a person refuses to co-operate and insists on leaving. In such circumstances, it may not be necessary to take the person to a police station: detention may be short …, for example to complete an examination."

13. The fact that detention is not used in the vast majority of cases where a Schedule 7 examination is considered necessary does not affect the correct construction of the powers since detention may be required. But it does show that usually the specific powers are not in fact needed. Most people would expect that they might be questioned at a port, particularly if seeking to enter the country. However, it does not in my view justify a wider scope being given to the exercise of the powers than is justified by the statutory language used. I would only say that I am not persuaded that the Code indicates or was intending to indicate the only circumstances in which detention would be applied. In the instant case, there is no suggestion that the claimant was other than co-operative, but, since the examination took just over 6 hours, he was detained. I suspect that will be the position with any lengthy need to examine. Paragraph 11 of the Code requires the officer to inform the person concerned that he is being examined under Schedule 7 and that there is power to detain if there is a lack of co-operation. After 1 hour, a form known as TACT1 must be served. This informs the person concerned that he is being questioned under Schedule 7 and what the officer's powers and his obligations are. He is also told that he can request that a friend is informed and that he can ask to consult a solicitor. It would, I think, be a little surprising, if the examination were likely to continue for any substantially longer time, that detention would not, even if demanded in the sense that the person concerned was unwilling to co-operate, be deemed necessary. However, that is not relevant to construction of the powers, but I shall have to return to it when considering a subsidiary ground of the claim relating to the claimant's request for advice from a solicitor.

14. Paragraphs 9 and 10 of the Code state:-

> "9. The purpose of questioning and associated powers is to determine whether a person appears to be someone who is or has been concerned in the commission, preparation or instigation of acts of terrorism. The powers, which are additional to the powers of arrest under the Act, should not be used for any other purpose.
>
> 10. An examining officer may question a person whether or not he suspects that the person is or has been concerned in the commission, preparation or instigation of an act of terrorism and may stop that person for the purposes of determining whether this appears to be the case …"

This guidance simply follows the provisions of sub-paragraphs 2(1) and (4) of Schedule 7. It emphasises that the only purpose of any examination must be to determine whether he is a terrorist within the meaning of s.40(1)(b). The existence of prior information suggesting that he is or may be a terrorist will not determine whether an examination can properly be carried out, but, as this case shows, the nature of that information may in a given case be determinative. In fact, as must be obvious, the existence of prior information is likely in many cases to mean that an examination will be considered to be necessary. But the officers are able to act on an intuitive basis even if no prior information exists.

15. The wording of s.40(1)(b) is important. It in my judgment recognises that it must be open to an officer to act under Schedule 7 to determine whether a person appears to be or to have been concerned and to identify any acts constituting that concern. Thus, even if it appears that he has in the past been concerned in any such acts, it is open to the officer to examine him to determine whether he is still so concerned. Equally, it may be apparent that he is concerned in acts against a foreign government, but it must be open to officers to examine him to determine whether his acts affect this country or, indeed, any country other than that affected by his known acts. In the end, Mr Otty Q.C. did not challenge that an examination would be lawful in circumstances such as these.

16. It in my view goes further than those obvious requirements which are essential to fulfil the purpose of the Schedule 7 powers, namely the protection of the inhabitants of this (or indeed any other) country from acts of terrorism. If officers are informed by the Security Service or from any other source that a person, who appears to be a terrorist, is suspected of possible involvement with others in a specific terrorist plot, they may examine him for the purpose of determining whether he appears to be so involved. This is because the language of s.40(1)(b) is wide enough to allow for examination not only of whether he appears to be a terrorist but also of the way in which or the act by which he so appears. The officer is not, unless the powers are to be ineffective in their purpose to protect from terrorism, prevented from examining a person even if it appears he is a terrorist in particular respects, for example if in the past or by acts only affecting a foreign government.

17. Mr Otty submitted that once it appeared to the officer carrying out the examination that the person concerned was or was not a terrorist, the examination must come to an end. There are difficulties with this submission. First, the determination is not necessarily one for the examining officer. For example, searches may have taken place or samples taken and examination of anything obtained may show that an apparent concern in the relevant acts was not correct. It may therefore be important that all relevant information is obtained. Secondly, the apparent concern may be of past or particular acts amounting to terrorism and it may be important to see how far such concern goes. Thirdly, there may be a stage at which the officer is persuaded that the person concerned is a terrorist but further examination may dispel that view. It must be for the officer to judge when the examination should come to an end. No doubt his conclusion will then be forwarded to his superiors and the Security Service to see whether surveillance is required or there is sufficient to arrest under s.41. The officer himself has the power of arrest under s.41, but I would suppose that he would not save in the clearest case exercise that power. It might be necessary if the officer were satisfied that the person concerned was a danger and needed to be kept in

custody, but that could sometimes be addressed by informing the Home Office who could then impose immigration or other controls.

18. Mr Otty was able to derive some apparent support from the Code for part of his submissions. In the notes for guidance on Paragraphs 9 and 10, this is said:-

> "An examination must cease and the examinee must be informed that it has ended once it has been ascertained that the person examined does not appear to be or to have been concerned in the commission, preparation or instigation of acts of terrorism."

In my judgment, this is misleading. There may come a point when the officer does consider that the examinee does not appear to be a terrorist, but his conclusion may not be shared by others and may, when what has emerged from the examination or any search is put together with other material which may, for example, be in the possession of the Security Service be shown to be wrong. Equally, further examination may show that the officer's view formed at a particular point was wrong. Again, in my view he must be able to ask all questions that he reasonably believes to be needed to enable him or others to reach the necessary determination.

19. It is to be noted that Paragraph 8 of Schedule 7 confers powers to search, 'for the purpose of determining whether [the person being examined] falls within section 40(1)(b).' This may prima facie suggest a higher hurdle for a search than that set out in Paragraph 2 of the Schedule. However, Paragraph 8 refers explicitly to the powers of an examining officer 'who questions a person under paragraph 2'. It would in my view be somewhat absurd if the same test were not applicable for the asking of questions and the powers of search. But if the officer has in his view grounds for pursuing an examination, in reality he would have the power and it would be lawful to search whether or not the words 'appeared to fall' were substituted.

20. The power of arrest arises if a constable has reasonable suspicion that a person is a terrorist. It may be thought that there is little difference between that state of mind and the appearance to the officer that the person is a terrorist. Mr Basu submitted that there is a difference and that it is possible for a person to appear to the examining officer to be a terrorist but for the officer not to have reasonable suspicion that he is. I am bound to say I find that supposed difference difficult to follow. But I do not think it matters since a power to arrest does not mean that there is an obligation to arrest. Furthermore, the officer may have reasonable suspicion based on his examination and any information he may have been given by the Security Service or from other sources. But he may be aware that a prosecution would not succeed because the evidence on which the reasonable suspicion is based cannot be deployed either because it cannot be divulged to the defendant since, for example, it would be contrary to the public interest to do so or because any admissions which might otherwise be relied on resulted from the obligation to answer questions put in the course of the examination under the Schedule 7 powers. In such circumstances an arrest would clearly be inappropriate. Schedule 7 powers are not conferred in order to enable an arrest to take place.

21. In the course of argument Mr Otty referred to paragraph 4 of Schedule 14 pointing out that it did not state that an examining officer could supply information acquired by

him to the Security services. Paragraph 4 is intended to enable information which relates to matters other than terrorism which has resulted from an examination to be passed on. For example, a search may produce material demonstrating a criminal offence such as drug or other smuggling or fraud. Paragraph 4(1)(a) enables information to be given to the Home Office which is relevant to immigration. An example would be a forged passport or answers given indicating that the person was not entitled to entry under the Immigration Rules. There is no need to specify who can receive information about terrorism, since it is obvious that the Security Service, the police and the Secretary of State are proper recipients. In any case, s.19 of the Counter-Terrorism Act 2008 enables relevant information to be given to the security service by anyone.

22. Having set out how in my judgment the Schedule 7 powers can properly be exercised, I turn to consider the facts of this case. The claimant is a British national who left this country in 2007 for Somalia. On 14 January 2011 he was arrested in Somaliland. He was interrogated and, he asserts, severely ill-treated during his interrogation. The authorities there decided that he should be deported to the United Kingdom. In anticipation of his return to the United Kingdom, on 13 January 2011 a control order was made against him pursuant to s.2(1) of the Prevention of Terrorism Act 2005. On 13 January 2011 Silber, J gave the Secretary of State permission to make the order.

23. In order to justify the making of a control order, the Secretary of State had to have reasonable grounds for suspecting that the claimant was or had been involved in terrorism related activity and had to consider that it was necessary for purposes connected with protecting members of the public from a risk of terrorism to make a control order. Thus there had to be reasonable grounds for suspecting that the claimant's terrorist related activities constituted a danger to the inhabitants of this country. Before making a control order, the Secretary of State must consult the police to ascertain whether the person concerned is the subject of a police investigation with a view to prosecution and, importantly, whether there is evidence available which could be used for the purpose of prosecution. The police response in this case was in the negative.

24. On 11 March 2011 the Security Service posted to the police at Heathrow a message stating that the claimant would be arriving at 6.35 am on 14 March 2011. This supplemented what is known as a Ports Circulation Sheet of December 2010 which referred to the claimant and set out a summary of what was known about him. This summary stated that the claimant was believed to have taken part in various extremist activities in Somalia, including terrorist training and facilitating the travel of persons from the United Kingdom to undertake terrorist training. It set out 28 questions which it was suggested should be included in any examination of him if he returned to the United Kingdom. At that time, it was not known when he would be returning nor had a control order been made. It was, however, clear that it was suspected that he was a terrorist.

25. The purpose of the message sent on 11 March 2011 was to request the assistance of the police in relation to the return to the United Kingdom of the claimant. It was said that the senders would be grateful if the police would consider using their Schedule 7 powers to 'interview [the claimant] and gain intelligence about his time spent in Somalia and recent travel to Somaliland'. They were asked in addition to consider carrying out searches of his person and any luggage he might have. It explained that

it was assessed that the claimant had been training in an Al-Qaeda camp and fighting for al-Shabaab and assisting extremists to travel to Somalia for terrorist training. Three named individuals were identified as his terrorist associates. It was said that he had been arrested on 14 January 2011 but the authorities had been unable to prosecute him and his associates there but the claimant was to be deported. There were then set out 118 questions which it was suggested should be asked if it was considered necessary to subject the claimant to a Schedule 7 stop 'to gain intelligence about his time spent in Somalia and his recent travel to Somaliland'. The police were asked in the message to 'make a full record of any complaints made by [the claimant] relating to his treatment in detention in Somaliland' but not to be drawn into any discussion regarding HMG involvement in his arrest. Interestingly, when asked about his treatment, he alleged serious ill-treatment but said he did not regard it as torture.

26. The officer who was responsible as Ports Duty Supervisor decided that the Schedule 7 powers should be used as requested. He explained the basis of his decision in his statement produced before me saying, in Paragraphs 7 and 8:-

> "7. The receipt of information such as above does not automatically result in officers exercising their Schedule 7 powers. For example, there have been occasions where a PCS may not be up to date and in such a case I would go back and question the originator. Furthermore, there have been cases where the request has been referred back to the originator to clarify information in order to assist me in carrying out my review. This includes cases where, for example, a stop has been suggested not long after officers have previously stopped a person. I understood the 11th March message to be a request, together with necessary information sharing, and the decision whether or not to exercise the Schedule 7 power was a policing decision.
>
> 8. The purpose for which people are stopped pursuant to Schedule 7 is to determine whether a person is, or has been, concerned in the commission, preparation or instigation of acts of terrorism ("CPI"). I can confirm that this is the purpose for which CC was stopped on 14th March 2011. However, as the public would expect, information is shared between the police and the U.K. intelligence services and that can result in intelligence led stops and it can involve the police being provided with information as to questions that may assist in determining whether the person stopped is or has been concerned in CPI."

27. Two officers carried out the examination. In Paragraph 4 of his statement, one of the two says this:-

> "Prior to stopping CC on the morning of the 14th March, [the other officer] and I received and read the information received … about him. I therefore knew that a Control Order had been made in respect of him and was due to be served on him when he arrived at Heathrow. Moreover, I accept that given what I had read about CC he *appeared* to be a person falling within

> s.40(1)(b) of TACT … However, I considered that the use of my powers under Schedule 7 was necessary and justified for the purpose of *determining* whether he was, in fact, someone who appeared to be [a terrorist]."

He records that the examination lasted for about 6 hours and that the claimant was co-operative and pleasant throughout. While the claimant said he did not regard his ill-treatment as torture, the officer felt it necessary to take the steps required if torture allegations were made having regard to the nature of the treatment described by the claimant.

28. Mr Otty made an application to cross-examine the two police officers whose statements were produced by the first defendant. The two issues which he said needed investigation by way of cross-examination were whether they had already determined that the claimant appeared to be a terrorist and whether the powers were exercised solely or predominantly not for the purpose of making such a determination but in order to provide information for the Security Service to use in the control order proceedings. Cross examination is rare in judicial review claims and is only allowed if there are factual issues which must be resolved if the claim is to be properly considered. That is not the case here. Mr Otty was able to assert that, even if they believed that they were entitled to exercise the Schedule 7 powers, in truth in the light of what they knew in advance and the nature of the request made by the Security Service they were not. Cross-examination would not have assisted, particularly as the good faith of the officers was not only not material if they were wrong but was not likely to have been established. Accordingly I refused the application.

29. It was accepted by the officers that the claimant did on the information available to them, in particular the existence of the control order, appear to be a terrorist. The request from the Security Service with the 118 questions was not likely to cast any doubt on that; quite the contrary. It was clear that the claimant was reasonably suspected not only to be a terrorist for what he had done in Somalia but was a danger to the inhabitants of this country. The request in terms was to gain intelligence about his time spent in Somalia and his travel to Somaliland. Thus there was no question of a determination being needed in respect of terrorism of a different nature to that which already appeared to exist.

30. Mr Otty submits that on the evidence the sole and certainly the predominant purpose of the examination was to provide information to the Security Service to assist it in the control order proceedings. The Security Service was aware that ill-treatment which might be regarded as torture had been alleged and so information obtained by the authorities in Somaliland might be inadmissible. It might help if questioning to which answers had to be given elicited any useful information.

31. Mr Basu submitted that the officers were entitled to question to find out more about the nature of his terrorism. Furthermore, since the determination did not have to be made by the examining officers (albeit the officer's statement rather suggests that it was his view that it was for them in the circumstances) any information might assist in establishing whether the view formed leading to the control order was correct. As I have already said, in principle how and the extent to which a person appears to be a terrorist can provide a lawful justification for a Schedule 7 examination.

32. However, all will depend on what the officers knew and why they decided to use their powers. Thus I do not doubt that they were entitled to establish that the claimant was indeed CC and the person the subject of the request from the Security Service, but that would not have involved more than a short examination. Beyond that, it is difficult to see what there was to determine since the Security Service and the police, who had been asked for their views pursuant to s.8 of the 2005 Act, had reasonable suspicion covering what he had done in Somalia and what he was expected to do in the United Kingdom if not subjected to a control order. The officer in Paragraph 4 of his statement accepts that the claimant appeared to him to be a terrorist from what he knew about him. His justification for the use of the Schedule 7 powers based on the need to determine whether he was in fact a terrorist is difficult to accept having regard to the questions which he was requested to and did ask.

33. While the officers may have asked a few questions which went beyond those 118 set out in the request, in essence they followed the script. As it happens, they got hardly anything of use since the claimant denied in some cases knowledge of and in all cases involvement in any terrorist activities with the various persons whose names were put in the questions in the request. In their report, the officers detail his allegations about his ill-treatment. While this might assist in the admissibility of evidence in the control order proceedings, it has nothing so far as I can see to do with the question whether he was a terrorist. When it was put to him that he was involved in al-Shabaab, it is recorded that, although he denied any such involvement, his "conversation and body language 'closed down'". The same applied when the name of a particular alleged terrorist with whom he had been, it was alleged, involved was put to him. This is said by Mr Basu to be of some significance and could help in the determination whether he appeared to be a terrorist.

34. I am afraid that I am satisfied that this was not a proper use of the Schedule 7 powers. It was clear that the Security Service for entirely understandable reasons was anxious if possible to get information which could not be regarded as tainted by any torture allegations or which might confirm the propriety of a control order. This had nothing to do with determining whether he appeared to be a terrorist in any particular way.

35. I have no doubt that this is a very rare case and that this decision will not damage the efficacy of the powers. They are properly given a wide construction for the reasons I have set out but cannot extend to the facts of this case.

36. I can deal briefly with further grounds which were raised in relation to a request made by the claimant for a solicitor. Paragraph 7 of Schedule 8 entitles a person detained at a police station to consult a solicitor. It is not clear to me why the Act limits the right to detention in a police station since, as this case shows, detention frequently will not be at a police station. It may, I suppose, have something to do with the knowledge that there are many ports in the country at which the powers can be exercisable. Some are remote and there may be unacceptable delays and difficulties if legal advice is sought save at a police station.

37. However, the TACT1 notice states that there is right to consult with a solicitor provided it causes no delay. The same information is given in the TACT2 notice but, once there is detention, it is said that a superintendent or above can authorise a delay. But each notice stated that such consultation or advice sought over a telephone would

not be at public expense. When informed of this, the claimant did not pursue the request since he said he could not afford to pay.

38. It is accepted that the notices were wrong in stating that access to a solicitor would not be at public expense. Albeit Schedule 8 Paragraph 7 limits the right to detention in a police station, it will continue to be permitted wherever the detention is taking place. There is nothing unlawful in the decision to go beyond what the Act specifically allows in the interests of fairness to the person being examined.

39. It is incidentally difficult to see what contribution a solicitor could usefully make since there is an obligation to answer questions put and to submit to searches and the taking of samples can occur in the circumstances set out. A solicitor could perhaps act as an observer to ensure proper procedure, but beyond that he would have nothing to do.

40. In the circumstances, it is unnecessary to say anything more about this aspect of the claim.

The real question about the terror suspect who fled in a burqa: did MI5 bring him here illegally?

Mohammed Ahmed Mohamed's escape was an embarrassment. The alleged torture and rendition that came before it might just be a major scandal

Ian Cobain
The Guardian, Wednesday 13 November 2013 18.40 GMT

Mohammed Ahmed Mohamed: snatched in Somalia by a team led by a man with a British accent, according to a fellow detainee. Photograph: Metropolitan Police/PA

The hunt was on from the moment that terrorism suspect Mohammed Ahmed Mohamed sliced off the electronic tag that was strapped around his ankle, donned a burqa and slipped away from a London mosque.

Within hours, the Home Office was announcing that a joint taskforce of police, Border Agency officials and MI5 officers had been ordered to track him down. According to some reports, undercover soldiers were also drafted in. One newspaper declared that Mohamed had "made a mockery" of the government's claim to protect the public, while another offered a reward for information leading to his capture: "£25k to Find the Burka Bunker".

Behind the headlines about the manhunt, however, lies another story. It is one that is a little less dramatic. But in the eyes of some, it is a story that is far more disturbing.

Mohamed was in Britain against his will: he had been forced aboard an aircraft in Somaliland, the breakaway territory in northern Somalia, and flown to the UK in March 2011 in an operation that his lawyers say amounted to little more than an act of rendition. He and a second man had been detained in Somaliland two months earlier and allegedly suffered severe mistreatment while they were being interrogated. Since then, evidence has emerged that the British government had a hand in their detention, and may have supplied many of the questions.

As a consequence, the coalition government is now facing, for the first time, serious allegations of complicity in rendition and torture. The men's accusations, if true, would appear to flatly contradict the assurances given by the heads of the three main intelligence agencies when they stepped out of the shadows for the first time last week, telling the intelligence and security committee they have learned a great deal since 9/11, and that "at this stage" their officers could not possibly become complicit in torture. However, the public may never learn whether the allegations are true or not: when Mohamed and the second man decided to sue the British government for damages, lawyers representing the intelligence agencies called upon the secret justice provisions of the highly controversial Justice and Security Act.

It is the first time that the government has resorted to these provisions since the act became law earlier this year. As a consequence of this move, any evidence that the government itself possesses that supports the allegations is unlikely ever to see the light of day. Instead, any such evidence will be heard by the court in secret, and part of the court's final judgment will also remain concealed.

Mohamed, 27, and the second man, a 25-year-old, are both British citizens of Somali descent. MI5 is satisfied that both are terrorists who are deeply involved with al-Shabaab, the group that carried out the attack on Nairobi's Westgate shopping mall in September.

While the two men deny this allegation, Mohamed is assessed to be linked to a group said to have received terrorism training from Saleh Nabhan, a leading al-Qaida figure suspected of involvement in the 1998 US embassy bombings in east Africa. He is also said to have received terrorism training and to have fought for al-Shabaab, and is accused of helping other British men slip into and out of Somalia, where his wife and two children live.

The second man can be identified only as CF since becoming subject to a Terrorism Prevention and Investigation Measure (TPIM) notice, introduced to replace control orders. He travelled to Somalia in 2009, where he too is said to have received training

and fought alongside al-Shabaab.

When Mohamed went on the run, Theresa May, the home secretary, said he did not pose "a direct threat" to the public. Nevertheless, MI5's anxieties about young British Muslims travelling to Somalia were made public in a speech given by the agency's then director general, Jonathan Evans, in September 2010. "I am concerned," he said, "that it is only a matter of time before we see terrorism on our streets inspired by those who are today fighting alongside al-Shabaab."

It appears that, in January 2011, CF wished to return to the UK via Addis Ababa, and asked Mohamed to help him travel across Somaliland and on to the Ethiopian border. On the night of 14 January, while staying in a house in the town of Burao, the pair heard a helicopter hovering overhead. Moments later, a group of armed and uniformed men burst through the front door, forced hoods over their heads and tied their hands tight behind their backs. CF claims he could hear the leader giving orders in English, with a British accent. At one point, the hoods were said to have been lifted briefly so that their faces could be checked against what appeared to be mugshots. Both men say they were fingerprinted and that DNA swabs were taken from inside their cheeks; CF says "Bravo 1" was written across his forehead.

Over the next few days, the two men allege, they faced mock executions and severe beatings, and were then held in brightly lit cells at a prison in Somaliland. CF claims he was kept naked for a period, and was once half-strangled with a piece of cloth. When a UK Foreign Office consular official visited CF a month after his detention, he recorded that marks, apparently from handcuffs, were visible on CF's wrists.

Both men also say they were interrogated repeatedly, and that they believe the questions were based on information that can only have been supplied by the British authorities. Meanwhile, the local media reported that their capture was the result of a joint operation by British and Somaliland intelligence officers.

On 13 March, the two men were taken from the prison to an airport, where they were forced aboard a flight to Dubai. Mohamed says he begged to be returned instead to Somalia, to be reunited with his family. In Dubai, they were put aboard another flight, to London, and guarded en route. Neither man was aware of any formal deportation process. The British government says the deportation was lawful under Somaliland law; the men's lawyers complain that they had, in effect, been rendered.


A CCTV image of Mohamed making his escape dressed in a burqa. Photograph: AFP

Since their forced return to the UK, evidence that the government was closely involved in the detention operation in Somaliland has seeped steadily into the public domain. First it became apparent that May had signed Mohamed's control order on 13 January 2011, the day before the pair were arrested. Then it became clear that in March that year, two days before the pair were taken from prison and forced aboard an aircraft, MI5 had sent an email to police at Heathrow giving precise details of the flight upon which the men would be arriving at the airport. The agency said it wanted Mohamed to be held and questioned under Schedule 7 of the Terrorism Act 2000 – the same measure that was used to detain David Miranda, the partner of former Guardian journalist Glenn Greenwald. MI5 had 118 questions it wanted to be put to Mohamed.

The email asked police to make a full record of any complaints he made about his treatment in Somaliland, but warned officers: "We would be grateful if you would NOT be drawn into any discussion with MOHAMED regarding HMG [Her Majesty's Government] involvement in his arrest." The email also showed that the agency was anticipating the possibility of being sued for damages over the affair: "You should be aware that any such write up is likely to be disclosable in any future civil proceedings."

After five hours of questioning at Heathrow, Mohamed was told he had been made the subject of a control order, and was compelled to go and live in the east of England – in a town where he knew nobody and where MI5 believed he would be far removed from his jihadist associates.

Later that year, the high court ruled that the police at Heathrow had abused their powers when they detained Mohamed. Schedule 7 permitted them to detain and question him only in order to help establish whether or not he was a terrorist: but the home secretary had determined that he was a terrorist two months earlier, when she signed his control order.

The purpose of holding Mohamed at the airport, despite the police not having the lawful power to do so, appears to have been in order to ask MI5's 118 questions. Mohamed says these were essentially the same questions that had already been put to him while he was being beaten and threatened with death in a jail in Somaliland.

His solicitor, Gareth Peirce, is highly critical of what she says was an attempt to clean up information that had previously been extracted under torture: "Schedule 7 was unlawfully deployed, and extended far beyond any legitimate legislative purpose to launder 'intelligence' obtained, equally unlawfully, from torture in Somaliland." While ruling that there had been improper use of Schedule 7 powers, the judge commented: "It was clear that the Security Service, for entirely understandable reasons, was anxious if possible to get information which could not be regarded as tainted by torture allegations or which might confirm the propriety of a control order."

In July last year, at the high court, while Mohamed was challenging his control order, the court heard that, a few weeks before the two men had been detained and forcibly removed to the UK, the Crown Prosecution Service had advised Scotland Yard there was insufficient admissible evidence to charge Mohamed with any terrorist offence.

An MI5 officer gave evidence at that hearing, and Mohamed's counsel, Tim Otty QC, asked him a series of questions. Had the agency been involved in Mohamed's detention in Somaliland? Did it accept that such an operation had no basis in law? Would MI5 acknowledge that it had "participated actively" in Mohamed's interrogation despite knowing he had suffered serious physical mistreatment? Had the agency been involved in his removal from Somaliland to the UK? Was it aware that CF had been beaten and subjected to a mock execution after his arrest?

To each of these questions, the MI5 witness gave the same reply: "I can neither confirm nor deny that."

An Noor Masjid and Community Centre in Acton, London, from where Mohamed slipped away in a burqa.

Photograph: Amer Ghazzal/Demotix/Corbis

Before the 2010 general election, a number of politicians who are now cabinet ministers quietly let it be known that they were horrified at the way in which the country's intelligence agencies had become involved in rendition and the mistreatment of terrorism suspects after 9/11, and that they were greatly concerned there appeared to have been ministerial approval. Within two months of the formation of the coalition, David Cameron signalled a change of direction when he announced that there would be an inquiry, and that the hitherto-secret policy that governed MI5 and MI6 "detainee operations" would be rewritten and made public.

Some sounded a note of caution. Sir John Sawer, the head of MI6, for example, pointed out in an unprecedented public speech that the agencies could not afford the luxury of working only with friendly democracies. "Dangerous threats usually come from dangerous people in dangerous places," he said. "We have to deal with the world as it is." But across much of Whitehall the sense of relief was almost palpable.

Three years on and the inquiry has been shelved amid a behind-the-scenes dispute about control of the evidence that was to be made public. An interim report from the inquiry has been sitting on the prime minister's desk for almost 18 months, despite a government pledge that as much as possible would be published. Four separate police investigations grind slowly on.

The intelligence agencies – and government ministers – are once again facing what Otty described in the high court last week as "core allegations of very grave misconduct". The Foreign Office and Home Office both told the Guardian that they were unable to comment on the allegations that the government now faces, precisely because of the ongoing proceedings in the civil courts. Government lawyers are indicating that they may attempt to have Mohamed's case struck out, on the grounds that it would be wrong for the courts to entertain such a claim while he is in breach of an order of the court by being on the run.

Almost two weeks after Mohamed disappeared, there remains no sign of him.

That still leaves CF's damages claim against the government. However, CF's solicitor, Ravi Naik, fears that the use of the secret justice measures of the Justice and Security Act will result in an odour of suspicion for ever lingering around the affair. "Our client could fail or succeed in his case without ever knowing why," Naik says. "This much is clear from the fact that the government has sought to put its entire defence into secret sessions.

"In those circumstances, our client – and the public – will for ever be kept in the dark about whether the British government was involved in serious wrongdoing."

Written evidence submitted by ARTICLE 19 [CT 19]

Re: Concerning the review of *The Guardian* newspaper as part of the inquiry into anti-terrorism

I am writing to you on behalf of the international freedom of expression group, ARTICLE 19, and leading civil liberties groups and campaigners in the UK, in relation to the Committee's review of *The Guardian* newspaper as a part of the inquiry into anti-terrorism.

We are deeply concerned that the Committee's review of *The Guardian* could restrict media freedom in the UK, by discouraging future reporting on important matters of public interest. This includes future reporting concerning the sensitive area of national security.

We also believe that the Committee's review of *The Guardian* raises concerns about the human rights of all individuals to be able to access information about government activities, and to be able to use that information to engage in public debate.

We write to you to ask that you consider this **an important opportunity to hear first-hand about the impact that pressure by the government and the security services has on the free press** when dealing with issues related to national security. Frequently, around the world, national security is used to justify arbitrary censorship and to curtail freedom of expression and press freedom. The international community are listening to the vigorous debate currently taking place in the UK that has been sparked by *The Guardian*. The voice of the Committee will be heard and will have influence beyond UK borders.

We, therefore, urge that **the Committee's review of *The Guardian* fully considers and takes into account international human rights standards, and in particular those that relate to the right to freedom of expression and media freedom**.

International standards on freedom of expression clearly stipulate that national security arguments must never be used to justify preventing disclosures of illegalities or wrongdoing, no matter how embarrassing such disclosures may be to governments. A summary of the relevant standards is outlined for your consideration in the enclosed Annex ("International freedom of expression standards relating to *The Guardian* newspaper's reporting of the Snowden disclosures").

In the present matter, *The Guardian* published information on large-scale internet and telephone surveillance programmes operated by the US Government with the assistance of the UK security services and a range of private sector internet and telephone companies. The publication of this information has facilitated a much-needed public debate about mass surveillance in a democracy. It also exposed the possible violation of the fundamental human rights of millions of people worldwide. We firmly believe that these matters fall within the public and political field which, according to the UN Human Rights Committee, necessitates special respect and requires the government to provide a particularly pressing justification for restrictions on freedom expression.

We observe that the UK government has so far failed to "specify the precise nature of the threat" relating to national security and has relied solely on a general statements referencing the concept of national security. General statements about the threat to national security do not meet established international standards on freedom of expression and media freedom, nor do they present a sufficiently justified pressing social need for such restrictions. The government has also failed to show that that there has been demonstrable harm to national security, and that this harm outweighs the public benefit derived from disclosures about mass surveillance and the potential violation of human rights.

We find that *The Guardian's* publishing of the Snowden disclosures relates not only to matters of great public importance, but is also directly concerned with reporting the human rights violations entailed in mass surveillance. As such, the most stringent journalistic protection is required.

We urge the Committee to uphold international standards on freedom of expression in the present review. **We respectfully call on you to unequivocally dismiss all allegations that the publishing activities of *The Guardian* have breached national security.** We strongly believe that any conclusion to the contrary would have a dangerous impact on human rights protection in the UK and would undermine the UK's international obligations.

We are further concerned that the Committee's review into *The Guardian's* activities further adds to an already unduly hostile environment for investigative journalism. We believe that sustained pressure is being applied to *The Guardian* by politicians and the authorities as a result of their reporting of the Snowden's revelations.

We would like to ask the Committee to be mindful that its approach to questioning *The Guardian* could bolster politically motivated pressure designed to curtail serious public interest journalism. It is for this reason that we ask you to defend and protect the right to freedom of expression and media freedom in the UK.

We would be very happy to further assist you in ensuring that the international standards are protected in the present review. Please do not hesitate to contact us should you need any further information.

Thomas Hughes, Executive Director, ARTICLE 19
Caspar Bowden, Independent Privacy Researcher
Henry Porter, Journalist, The Guardian
Susan Bryant, Director, Rights Watch (UK)
Jo Glanville, Director, English PEN
Jim Killock, Executive Director, Open Rights Group
Dr Ian Brown, Associate Director, University of Oxford Cyber Security Centre and Senior Research Fellow, Oxford Internet Institute
Anthony Barnett, Founder, Open Democracy

December 2013

Annex

International freedom of expression standards relating to The Guardian newspaper's reporting of the Snowden disclosures

The right to freedom of expression under international law

The right to freedom of expression is protected under international and European law. Notwithstanding its importance, the right is not absolute and may be restricted in certain limited circumstances.

Under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), restrictions on the right are permitted, *inter alia*, to ensure the protection of national security or public order (*ordre public*). However, when a State party imposes restrictions on the exercise of freedom of expression, these restrictions should not jeopardise the right itself.

The UN Human Rights Committee has indicated that the relationship between right and restriction, and between the norm and the exception, must not be reversed.[i]

Article 19(3) also lays down specific conditions, and it is only subject to these conditions that restrictions may be imposed (the "three part test"):

- The restrictions must be "provided by law;"
- They may only be imposed for one of the grounds set out in Article 19(3)(a) or (b) of the ICCPR; and
- They must conform to the strict tests of necessity and proportionality.[ii]

Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated.

Similar requirements are illustrated and elaborated in the case law of the European Court of Human Rights.

Under the above standards the need to protect national security may warrant restriction upon an individual's freedom of expression, but only if such a limitation is, *inter alia,* **"necessary" for a legitimate purpose in the sense that there must be a "pressing social need" for the restriction**.[iii]

The principle of proportionality also has to be respected in the sense that any restriction "must be the **least intrusive measure to achieve the intended legitimate objective** and the **specific interference in any particular instance must be directly related and proportionate to the need on which they are predicated**."[iv] All authorities must respect the principle of proportionality when applying the restrictions.

<u>Limiting the right to freedom of expression on the grounds of national security</u>

While there is a no universal definition of national security, there has been extensive development on the scope and boundaries of the concept by UN bodies and experts in the past two decades.

We note that these elaborations have taken a narrow view of the scope of the concept of "national security." As a preliminary matter, the UN Human Rights Committee has found that states must **"specify the precise nature of the threat"** relating to national security **rather than relying on a general statement of the concept**.[v]

In General Comment No. 34, the Human Rights Committee explicitly stated that:

> Extreme care must be taken by State parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition

> laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to **suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists**, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. [vi] [emphasis added]

The Siracusa Principles on the Limitation and Derogation of Provisions in the ICCPR further sets out circumstances in which national security can legitimately apply: [vii]

> 29. National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.
>
> 30. National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order.
>
> 31. National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exists adequate safeguards and effective remedies against abuse.
>
> 32. The **systematic violation of human rights undermines true national security and may jeopardize international peace and security. A state responsible for such violation shall not invoke national security as a justification for measures aimed at suppressing opposition to such violation or at perpetrating repressive practices against its population**. [emphasis added]

The UN Special Rapporteur on Promotion and Protection of the Right to Freedom of Opinion and Expression also set out his expert view on limitation in his report to the Commission on Human Rights in 1994:

> For the purpose of protecting national security, the right to freedom of expression and information can be restricted only in the most serious cases of a direct political or military threat to the entire nation.[viii]

The Special Rapporteur, in cooperation with the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, issued a special declaration on freedom of information in 2004, stating:

> Certain information may legitimately be secret on grounds of national security or protection of other overriding interests. However, secrecy laws should define national security precisely and indicate clearly the criteria which should be used in determining whether or not information can be declared.[ix]

The definition of national security has also been further developed by the Johannesburg Principles on National Security, Freedom of Expression and Access to Information:[x]

> (a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
> (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.

As described above, states must show that a restriction on freedom of expression on national security grounds is necessary. Principle 15(1) of the Johannesburg Principles elaborates on this requirement by stating that **"no person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest."**

Additionally, the UN Special Rapporteur on Freedom of Opinion and Expression, in his 2012 report reiterated that[xi]

> Journalists should not be held accountable for receiving, storing and disseminating classified data which they have obtained in a way that is not illegal, including leaks and information received from unidentified sources.

Further, the UN Special Rapporteur on Freedom of Opinion and Expression the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, in the declaration on freedom of information explicitly stated that:

> Public authorities and their staff bear sole responsibility for protecting the confidentiality of legitimately secret information under their control. Other individuals, including **journalists and civil society representatives, should never be subject to liability for publishing or further disseminating this information, regardless of whether or not it has been leaked to them, unless they committed fraud or another crime to obtain the information**. Criminal law provisions that don't restrict liability for the dissemination of State secrets to those who are officially entitled to handle those secrets should be repealed or amended.[xii][emphasis added]

[i] See Human Rights Committee, General Comment No 27, Freedom of Movement (Article 12), CCPR/C/GC/21/Rev.1/Add.1, 2 November 1999, para 13.
[ii] See Human Rights Committee, Communication No 1022/2001, *Velichkin v Belarus*, CCPR/C/85/D/1022/2011, Views adopted on 20 October 2005.
[iii] *Handyside v United Kingdom*, Eur Ct HR, Application No 5493/72, Series A No 24, Judgment of 12 December 1976, 1 EHRR 737, at para 48.
[iv] Human Rights Committee, General Comment No 22, Freedom of Thought, Conscience and Religion (Article 18), CCPR/C/21/Rev.1/Add.4, para 8.

[v] *Keun-Tae Kim v. Korea*, Communication No 574/1994, UN Doc. CCPR/C/64/D/574/1994 (4 January 1999), para 12.4.

[vi] Human Rights Committee, General Comment No 34, Freedoms of Opinion and Expression (Article 19), CCPR/C/GC/34, 12 September 2011.

[vii] UN Commission on Human Rights, The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN.4/1985/4.

[viii] Mr. Abid Hussain, Report of the Special Rapporteur on Promotion and protection of the right to freedom of opinion and expression, UN Doc. E/CN.4/1995/32, 14 December 1994, pp 48.

[ix] International Mechanisms for Promoting Freedom of Expression, Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2004.

[x] Endorsed by the Report of the Special Rapporteur, Promotion and protection of the right to freedom of opinion and expression, UN Doc.E/CN.4/1996/39, 22 March 1996, para. 154; Commission Res. 1996/53; Gamini Athukoral "Sirikotha" and Ors v. Attorney-General, 5 May 1997, S.D. Nos. 1-15/97 (Supreme Court of Sri Lanka) and Secretary of State for the Home Department v. Rehman [2001] UKHL 47 (House of Lords).

[xi] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (2012), UN Doc.A/HRC/20/17, [107] and [109].

[xii] International Mechanisms for Promoting Freedom of Expression, Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2004. This was reaffirmed in the 2006 joint declaration of the three special rapporteurs.

Written evidence submitted by Quilliam [CT 20]

THE LIMITATIONS OF TERRORISM PREVENTION AND INVESTIGATION MEASURES

ABOUT QUILLIAM

Quilliam is the world's first counter-extremism organisation, set up in 2008 by leading former extremists. It is a not-for-profit private company in the United Kingdom (UK) and incorporated as a 501(c)(3) organisation in the United States of America (USA). At present, Quilliam has ten full-time staff members and three volunteer interns.

At Quilliam we recognise that, not being merely a legal or military challenge, extremism and terrorism are now firmly entrenched social phenomena stripping away social, economic, political, civil and cultural rights for many societies across the world. We believe that the key to preventing the conflict and injustice caused by extremism and terrorism is worldwide social change led by civil society itself. We aim to bring about this change by engaging, educating and encouraging civil society to make their own strategic civic interventions which are able to challenge intolerant extremist narratives and instead advocate a more peaceful and just world for all. Quilliam seeks to challenge what we think, and the way we think. It aims to generate creative, informed and inclusive discussions to counter the ideological underpinnings of terrorism, while simultaneously providing evidence-based recommendations to governments for related policy measures.

The following is written evidence as requested by the Rt. Hon. Keith Vaz MP in his capacity as Chair of the Home Affairs Select Committee to review the policy of Terrorism Prevention and Investigation Measures (TPIMs) and their implementation.

TERRORISM PREVENTION AND INVESTIGATION MEASURES

The situation in the United Kingdom is admittedly more positive than in many places in the world, yet the threat of terrorism and the extremist ideologies and narratives that aim to legitimise it are still prevalent and must be addressed. Any response should be well-rooted in the universal human rights that underpin the liberal and democratic values we seek to protect and any component of counter-terrorism or counter-extremism must not further complicate other components of the effort. Quilliam believes that democracy will only defeat extremism by killing it softly, not by mimicking it.[1] It is widely accepted that "we cannot use force everywhere that a radical ideology takes root"[2] and we welcome the fact that the neo-conservative wars of George Bush jnr to instill democracy at the barrel of a gun, replaced by the neo-conservative-lite measures of Barrack Obama that treat al Qaeda as a mafia-style organisation and aim to decapitate its leaders through drone strikes, are now finally being complemented by a ten-year effort to counter violent extremism. Just as the former control orders were dismissed for being incompatible with human rights, Terrorism Prevention and Investigation Measures (TPIMs) also face accusations of being control orders-lite,

[1] Quilliam Policy Briefing, The Need for a Clear and Consistent Counter-Extremism Strategy Headed by an Expert to Steer the Prime Minister's Task Force, 4 June 2013, http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-need-for-a-clear-and-consistent-counter-extremism-strategy.pdf [accessed 20 January 2014]

[2] President Barack Obama at National Defense University Fort McNair Washington, D.C. 23 May 2013, http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university [accessed 20 January 2014]

rebranded for political capital.[3] However, it is here argued that TPIMs, if brought further into line with human rights and integrated with counter-extremism methods including challenging extremist ideology and narratives, can be a successful component of the current efforts to counter terrorism and counter extremism. Any assessment must, therefore, be both of the measures in isolation and as part of a larger agenda.

The need for measures to deal with individuals whom officials assess to be involved in terrorism-related activities but deem unable to charge or deport is valid. These British citizens will not have committed the "use or threat of action designed to influence the government or an international governmental organisation or to intimidate the public, or a section of the public; made for the purposes of advancing a political, religious, racial or ideological cause."[4]

The Terrorism Prevention and Investigation Measures Act 2011 is a welcome amendment that repeals and replaces the Control Orders in the Prevention of Terrorism Act 2005. It thereby ensures greater compatibility with the ECHR and less intrusion on the human rights of the individuals subject to them than the previous control orders, particularly in reference to the potential forced relocation and indefinite length of the control orders that have now both been written out of the revised TPIM legislation.[5] However there remain several significant problems with TPIMs that mean they are inconsistent with a clear human rights-based counter-extremism strategy and we hereby argue that the following further amendments need to be implemented in order to strike an appropriate balance between national security and civil liberties:

> 1) Currently, someone subject to a TPIMs notice will not face a fair trial, has no opportunity to present evidence to show their innocence, nor has the right to appeal. The British traditions of justice and liberty must be upheld, not least because failing to do so feeds into false extremist narratives. While evidence collected by MI5 may not be appropriate for the traditional criminal justice system, there should be the possibility in the TPIM legislation for fair trial with the presumption of innocence and subsequent review or appeal. The addition of a legal representative for the suspects would help mitigate potential mistakes made by the authorities and would support vulnerable people as well as make the system more transparent and in line with the criminal justice system without compromising national security.
>
> 2) TPIMs must have an additional element that comprises deradicalisation, rehabilitation and reintegration where appropriate. In the current situation, someone subject to a TPIMs notice is under surveillance and investigation for a period of up to two years, often requiring reporting to a police station and with restrictions on movement, financial assets and association. These negative measures may be deemed necessary on a case-by-case basis, but are a blunt instrument if implemented for two years then lifted immediately thereafter unless new evidence emerges of involvement in terrorism. A suspect may commit a terrorism related offence once the TPIMs notice is lifted and the authorities would be unable to prevent such an action unless its planning was identified by the surveillance and

[3] D. Anderson, "TERRORISM PREVENTION AND INVESTIGATION MEASURES IN 2012", https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2013/04/first-report-tpims.pdf, 2013 [accessed 19th January, 2014].

[4] Section 1, TERRORISM ACT 2000

[5] TERRORISM PREVENTION AND INVESTIGATION MEASURES (TPIM) BILL, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/98372/echr-memorandum.pdf, [accessed 19th January, 2014]

investigation team. TPIMs punish suspected intent but do nothing to challenge this intent as there is no element that challenges the ideology or narratives that may support this intent. By integration of these measures with Channel projects or by developing new deradicalisation theories and processes to engage with suspects, not only will it be easier to ascertain a truer sense of an individual's intent to commit a terrorism related offence, it will also help prevent future acts of terrorism once the two year expiry date has passed without the need for further negative measures. Given that movement and association are already limited under TPIMs, the addition of pastoral visits would be a welcome addition.

Two high profile abscondences of those under TPIMs notices have called into question the effectiveness of the measures. While particular details of these two cases are unavailable and commenting on the ability of the authorities to monitor individuals is unnecessary, it must be noted that engaging with and rehabilitating the suspects coupled with a renewed commitment to the rule of law on the part of the authorities, even in terrorism related cases, may help to prevent such situations. This can be achieved by providing incentives related to the reinstating of personal freedoms, may remove the desire to abscond through the provision of rehumanising pastoral care and may restore a suspect's faith in alternative non-violent methods for advancing political, religious, racial or ideological causes within the confines of the law. Likewise, such provisions will also avoid further problems created by the ineffective current system where suspects who are considered too dangerous to be left uncontrolled one day are relieved of the measures the next day for administrative reasons without any clear ideological change.

If TPIMs must be kept, they will be limited or no use unless combined with a human rights-based, civil society-supported and joined up approach to countering extremism that includes the challenging of ideological narratives, deradicalisation, rehabilitation and reintegration at every stage of the criminal justice system.

As we advised the Task Force on Countering Extremism that was set up after the Woolwich attacks:

After this government's much needed 2011 reform of its Preventing Violent Extremism Strategy (Prevent), the counter-terrorism brief was rightly split from the work on integration and social cohesion. Whereas the Office for Security and Counter-Terrorism (OSCT) at the Home Office maintained its counter-terrorism portfolio, the Department for Communities and Local Government (CLG) took on board the integration and challenging extremism remit. Eight months after this 'Prevent' reform, CLG finally published its 'integration' strategy, indicating that a separate plan to 'outflank extremism' would be forthcoming. Eighteen months went by – until the murder of Drummer Lee Rigby - and no plan to 'outflank extremism' had yet been issued. In light of recent events therefore, it is imperative that the British Government urgently revisits and reclaims responsibility for developing a joined up counter-extremism strategy to challenge the rising threat of extremisms in the UK[6].

By way of a joined up counter-extremism strategy, we recommend the establishment of a permanent office led by counter-extremism experts, either elected or unelected, acting in a non-partisan capacity to ensure that the strategy is clear and consistent at judicial, policy and grassroots levels. A permanent office would avoid problems stemming from a lack of continuity, keep the debate above party politics and would ensure that there is an independent and expert source of

[6] Quilliam Policy Briefing, The Need for a Clear and Consistent Counter-Extremism Strategy Headed by an Expert to Steer the Prime Minister's Task Force, 4 June 2013, http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-need-for-a-clear-and-consistent-counter-extremism-strategy.pdf [accessed 20 January 2014]

advice for public officials at every stage of the criminal justice system. If TPIMs are to continue, this office can act as an independent reviewer of all individual cases, provide official deradicalisation and pastoral oversight to the suspects and ensure that a doctrine of “legal tolerance” is adhered to when dealing with extremist views while promoting a doctrine of “civil intolerance” by implementing counter-extremism training and education at a grassroots level.

We anticipate that the need for TPIMs will increase as the conflict in Syria continues as ever more British Muslims are drawn to fight alongside Al Qaeda-affiliated groups in Syria. While it is possible to charge returning British jihadists using the traditional criminal justice system as they have committed a crime by affiliating with a proscribed terrorist organisation, those with the intent to fight will be difficult to prosecute and TPIMs notices are most appropriate to prevent future acts of terrorism either in the United Kingdom or against British interests abroad. However, we urge that our recommendations for a human rights-based and rehabilitative approach are integrated into TPIMs in order to maintain and improve the effectiveness of these measures.

Quilliam
January 2014

Supplementary written evidence submitted by
Sir Anthony May, Interception of Communications Commissioner [CT 21]

Re: Supplementary evidence to oral session on 11th February 2014

Thank you for the opportunity to give evidence to your Committee yesterday. There were a number of questions that, due to time constraints, we were unable to answer fully on the day and therefore please accept this follow up letter as an extension of my evidence.

Does the ISC have access to the confidential annex of your annual report?

The previous report (covering 2012) was my predecessor's (Sir Paul Kennedy). I attended a meeting with the ISC in February 2013 during which the confidential annex was discussed. It is the Prime Ministers role under Section 58(7) to decide what material (if any) is excluded from the report laid before Parliament and to whom that material should be shared. I expressed no objection to the ISC receiving a copy of the annex, so long as this was sanctioned by the Prime Minister.

The ISC have confirmed today that their Chairman, Sir Malcolm Rifkind wrote to you on 6th February 2014 on this point and confirmed that the ISC has had access to all of the material in the Commissioners' annexes that falls within its remit. The Prime Minister agreed to this in a letter to the ISC in July 2013.

I am in the process of writing my first annual report to the Prime Minister which will cover 2013. My ambition is to not have a confidential annex. If I were to have a confidential annex, I would have no objection to the ISC being provided with a copy.

My predecessors have provided more and more information in successive annual reports in relation to our oversight regime, how we go about conducting our inspections, the outcomes of those inspections, the errors reported etc. This information is openly available for any member of the public to read if they choose to do so. I am hoping to be able to provide further information on our lawful interception oversight this year and I intend to address some of the Snowden related revelations.

Specifically how many communications data authorisations were examined in 2012? Are my resources adequate?

I was not appointed until 1st January 2013.

My oversight function is post facto - it is not a pre-authorisation regime. However in the smaller public authorities (such as local authorities) the inspectors do generally examine 100% of the applications submitted in the period being examined.

We have looked at how many applications are examined during the inspections of police forces and other large volume users recently for my 2013 annual report and estimate that the inspectors look at between 5-10% of the applications submitted in the period being examined (which is now annually for the larger users).

It is difficult to be exact about the percentage of applications randomly sampled as the number of applications submitted is not reported to my office in the annual statistics. The number of applications submitted will obviously be significantly less that the number of notices and authorisations, due to the fact that the majority of applications will contain multiple requests. In the larger volume public authorities sampling must of course be undertaken. It is worth pointing out a number of things;

- The random sampling is conducted at both ends of the process – i.e. from the public authority records and the data obtained from the CSPs.

- If the Inspectors identify an error / issue during the random sampling which may impact on other applications, the public authority is tasked to identify the other applications which contain the same error / fault. Therefore, although random sampling may only pick up 1 error, this will lead to all error instances of that type being investigated and reported.

- The Inspectors have full access to the computer systems used by the larger volume users and interrogate those systems.

- In addition to the random sampling, the Inspectors also conduct query based searches across the systems. The query based searches ensure that a cross section of applications are examined; covering all data types and necessity purposes; a variety of applicants, SPoCs and designated persons; various priority grades; urgent oral requests; referrals / rejections; any particularly intrusive requests; any errors.
- The Inspectors will continue to examine applications until they reach the point that they are satisfied that what they have examined is an accurate representation in relation to the public authority's level of compliance. Compliance is measured against the inspection baselines which are drawn from the Act and Code of Practice (CoP).

I am satisfied that the random and query based sampling gives a reliable picture.

I have recently recruited 3 additional inspectors on the communications data side of the business and I am satisfied that my office is sufficiently resourced in this area. I have requested a further inspector on the lawful interception side of the business and this post has recently been agreed.

Are the statistics adequate and could they be broken down in your annual report further?

This is difficult on the interception side of the business for obvious reasons.

On the communications data side of the business I think that more could be done. My predecessor hinted at the inadequacy of the statistical requirements in the Communications Data Code of Practice in his 2012 report. I can report that my office has been engaging with the Home Office for some time with a view to enhancing the statistical information that public authorities are mandated to collect. The vehicle for these changes was going to be the communications data bill (revised code of practice).

The statistical information is flawed at present as it only requires the number of authorisations and notices to be reported. More than 1 item of data may be requested on an authorisation or

notice – and different systems in use by public authorities have different counting mechanisms. This makes it very difficult to draw accurate and meaningful comparisons. If further breakdowns are provided, we are in danger of misleading the public if the appropriate caveats are not applied to the data.

I believe that more statistical information should be available in relation to the statutory necessity purposes under which data is acquired. As the public authorities are not mandated to provide this information, their systems have not been designed to easily extract the data – it would be impractical to ask the larger volume users to count thousands of requests manually. However, my office has conducted a scoping exercise for the 2013 annual report and is hoping to be able to provide some further statistical information on this point (and others) - but it is likely that the statistics will be a representative sample rather than a complete picture.

We are aware that a number of CSPs are releasing transparency figures in relation to the disclosures they make to law enforcement. These statistics should be treated with caution as different counting mechanisms and rules are applied which means you are essentially comparing apples with pears. This could be misleading. In our view the statistical information should be collected by the public authorities. The Home Office should agree conventions and counting mechanisms with the public authorities to ensure that the statistical information is comparable and accurate.

Publishing of Investigatory Powers Tribunal (IPT) statistics / cases

You asked a question in relation to my office publishing IPT statistics.

I have looked into this in more detail and can report that previous Interception Commissioners Annual Reports (up to and including 2009) did indeed publish statistics and information in relation to the IPT. I am informed that this was due to the fact that the IPT did not have its own annual report and that prior to RIPA the Interception Commissioner's reports would have included details of the interception complaints made to the former tribunal systems. This is no longer the case. I can confirm that my office is separate to the IPT and has no access to any information in relation to the tribunal's work.

Finally, I note that the article in the Guardian on Tuesday evening *("Number of data interception requests to GCHQ possibly too large, says official"* by Ewen MacAskill and Richard Norton-Taylor) has misquoted a comment I made in relation to the 570,000 **communications data** requests**.** The 570,000 requests are **not** interceptions, but are requests for communications data under Part I Chapter 2 of RIPA and they of course relate to **all** public authorities – more than 200 in all – who acquire communications data.

I hope you find this additional information helpful. Please do not hesitate to contact my office if you require any further assistance.

Sir Anthony May,
Interception of Communications Commissioner

Written evidence submitted by the Ministry of Defence [CT 22]

Letter from Rt Hon Mark Francois MP, Minister of State for the Armed Forces, to the Chair of the Committee, 21 February 2014

I am writing in reply to your letter of 27 January 2014 to the Permanent Under Secretary for Defence, Jon Thompson, regarding the Defence Advisory Notice System. You wrote in the context of the Home Affairs Committee's inquiry into Counter Terrorism. I note that you requested a reply by 10 February 2014 and I apologise for the delay in my response; as I am sure you will appreciate however, Ministers have been very busy directing flood relief operations.

I must begin by explaining that the current Defence Press and Broadcasting Advisory Committee (DPBAC) has served the nation in various forms for around 100 years. Its function within the national security landscape is to provide a clear single source of advice and guidance to the UK media on handling information so as to prevent inadvertent public disclosure that would compromise UK military and intelligence operations and methods, or put at risk the safety of those involved in such operations, or lead to attacks that would damage the critical national infrastructure and/or endanger lives.

The DPBAC has a small secretariat (led by retired Air Vice Marshal Andrew Vallance). The committee itself is made up of, on one side, senior representatives of the UK print and broadcast media, and on the other, senior officials from relevant Government Departments. The Permanent Under Secretary of the MOD is the DPBAC chair; the Vice Chair is drawn from the media representatives on the committee. The secretariat is effectively the single point of contact between the media on the one hand and Government Departments and the Security Services on the other, when there are concerns about current or future media coverage within scope of the DA Notices.

The activity of the Committee solely concerns the five 'standing' DA-Notices. It should be noted that these are purely advisory; they carry no legal weight and cannot be 'enforced'.

The topics covered by each notice are as follows:

- DA-Notice 01: Military Operations. Plans & Capabilities
- DA-Notice 02: Nuclear & Non-Nuclear Weapons & Equipment
- DA-Notice 03: Ciphers & Secure Communications
- DA-Notice 04: Sensitive Installations & Home Addresses
- DA-Notice 05: United Kingdom Security & Intelligence Services & Special Services

Full details of the advisory scope for each notice can be found at the following web page: http://www.dnotice.org.uk/danotices/index.htm

The daily activities of the DPBAC secretariat are largely reactive, responding to contact from the media, academics, Government Departments, international bodies and any other approaches. On occasion the Secretariat does issue 'advisory messages' to all UK editors to alert them to DA-Notice implications in stories which are about to break or have broken. Typically 4-6 such advisory messages might be issued in each 12-month period, though in the most recent period ending November 2013 there were only two.

Since November 2008, the DPBAC's secretary and his deputies have responded to, on average, 266 requests every 12 months. The number of requests varies, reflecting the changing level of interest in areas of national security in the media. For example, requests over this period peaked at 357 in the 12 months ending November 2011; the main driver here was media interest in UK operations concerning Libya (Op ELLAMY).

Feedback from the UK media is expressed primarily through the DPBAC media representatives at the bi-annual DPBAC meetings. I judge they are broadly supportive of the current system, and I believe that in the vast majority of cases the UK media do seek advice from the DPBAC secretariat where they are in doubt about the impact of publishing material, and then follow the advice that is given.

I am also aware of recent publications in the print media about DPBAC, including an article by former Guardian editor Peter Preston in the Observer and the publication of a letter from retired Rear Admiral Nick Wilkinson (DPBAC Secretary 1999-2004) in the Times, both of whom were supportive of the current system.

I do however think the time is right to review the ownership, remit and effectiveness of the DA Notice system and the DPBAC, given that the media operate 24/7; are increasingly global both in origin and reach; now include extensive use of social media; and where many of the cases now addressed by the DBPAC relate to wider national security matters rather than the narrower field of defence alone. The terms of reference of the review are currently being developed and will be shared with stakeholders in due course.

I hope your Committee will find this information useful.

Rt Hon Mark Francois MP, Minister of State for the Armed Forces
February 2014

Written evidence submitted by
Sir Mark Waller, Intelligence Services Commissioner [CT 23]

Following our telephone conversation and your letter of 20th January 2014 I have (as I promised I would) reconsidered your invitation to give oral evidence before the Home Affairs Select Committee.

I am afraid I remain of the view that it would not be appropriate for me to do so. As my office informed you previously my function is limited to oversight of the intelligence services which is within the remit of the Intelligence and Security Committee (ISC) who as was explained have broadened their inquiry into privacy and security to consider the "appropriate balance between our individual right to privacy and our collective right to security".

In any oral evidence before your committee I could not go further than anything which is in my open report. The position is quite different before the ISC who are able to receive a wide range of sensitive material. The fair and appropriate place for questions to be put to me is before that committee.

There are certain matters raised in your letter on which I am happy to provide information.

1. My role is independent of the Interception of Communications Commissioner, the Investigatory Powers Tribunal (IPT) and the ISC. So far as the IPT is concerned my duty is simply to provide assistance and advice if asked (see section 59(3) of the Regulation of Investigatory Powers Act 2000}. I have only been asked on one occasion during the previous three years as set out on page 14 of my Annual Report for 2012. I appear once a year to discuss my Annual Report and other matters with the ISC.

2. My resources have varied during the previous three years. At present I have a full time personal assistant and we are in the process of recruiting further personnel.

3. I am not fully enough informed to provide a meaningful comparison between my oversight regime and that in other parts of the world.

4. As regards errors and my auditing these are the very areas which are covered in my open report so far as I am able. If you or any member of your committee have concerns in these areas I would encourage you to register those concerns with Sir Malcolm Rifkind and I will help him and his committee so far as I am able.

Sir Mark Waller,
Intelligence Services Commissioner
18 February 2014

Supplementary written evidence submitted by the Metropolitan Police [CT 24]

Letter from Alison Duncan-Mercy, Head, ACSO's Strategic Briefing Unit, to the Chair of the Committee, 26 February 2014

HASC INQUIRY INTO PURSUE - FOLLOW UP QUESTIONS

1. Thank you for your letter to me dated 6 January, in which you asked a series of questions following evidence given by the Commissioner and Assistant Commissioner, Specialist Operations to the Home Affairs Committee on 3 December as part of its inquiry into Pursue. I am responding on their behalf.

Inquiry in to "The Guardian "

Question 1. The number of officers who are working on the scoping inquiry, which is looking at whether *The Guardian* may have committed a crime in relation to the Snowden papers?

2. The MPS began a criminal investigation following the seizure of highly sensitive material during the detention of Mr Miranda under Schedule 7 at Heathrow Airport on the 18 August 2013. As part of our investigation we are examining the material to establish whether and what offences may have been committed which should determine what, if any, action should be taken.

3. The material seized was extensive and because the investigation is ongoing it would be inappropriate for us to discuss which individuals may be under investigation. We are continuing to work closely with the Crown Prosecution Service on this matter. The number of officers working on this investigation has varied according to the nature of the enquiries at each stage and will continue to do so as the investigation continues so it would be misleading to give a precise number.

Terrorism cases held in closed material proceedings

Question 2. Whether any other criminal cases have previously been held under a secrecy order as recently applied for in the trial of AB and CD?

4. The police and the Counter Terrorism Division of the CPS are unaware of any other anonymity orders granted in relation to defendants in other counter terrorism cases. As far as we are aware the matter is unique and this is not the normal course of events. Section 4(2) orders, restricting matters that can be reported, are reasonably common in counter terrorism court cases.

5. It may be worth clarifying that the orders in this case are temporary and may be lifted by the court in future as the need expires. At this stage decisions are yet to be made whether to apply to the court asking for the trial, or parts of the trial, to be heard in camera or for further reporting restrictions.

Foreign Fighters

Question 3. ***Are social media such as "Twitter" and "Facebook" being monitored for people who are claiming to engage or have engaged in fighting abroad?***

6. When we receive intelligence or evidence that suggests a person is fighting abroad we will naturally seek to develop it. Social Media is one aspect of enhancing an intelligence and evidential picture and it is normal practice to look at open source material as part of an investigation.

7. The CT police network has a national unit, the Counter Terrorism Internet Referral Unit (CTIRU) that conducts work in this area. This unit can assess the online social media content relating to an individual to determine whether any offences have been committed and to assist in the development of an investigation. However, because of the vast quantity of social media our focus in this area needs to be intelligence led.

Question 4. ***There have been claims that there is significant "coming and going" from the battlefield with people going to fight for a month or two in Syria and then returning to Britain to rest and recuperate. What legislative means does the Government have at its disposal to stop people returning to Syria? And is the legislation sufficient?***

8. As the HASC will be aware the issue of "Foreign Fighters" travelling to Syria is a major concern for the Government, law enforcement and our security partners and we are working closely to understand better the scale of the problem and to ensure we have the appropriate means to tackle it.

9. Depending on the intelligence or evidential case there are existing laws that can assist in the prevention of travel. However, it is important to highlight that where intelligence is limited we may be unable to meet the required thresholds for exercising powers available to us. Clearly where there is strong intelligence or evidence, powers of arrest under TACT 2000 can be used in order to investigate terrorist offences and establish whether individuals are engaged in the commission, preparation and instigation of acts of terrorism. In addition those seeking to travel may also reach the arrest threshold for criminal offences; such arrests may prevent or disrupt travel.

10. In terms of specific legislation aimed at curbing travel the following are most relevant at this time; TPIMs, foreign travel restriction orders, the Royal Prerogative, deportation, exclusion and deprivation. TPIMs require a strong national security case. Foreign travel restriction orders are available in relation to convicted terrorists who have received a sentence of imprisonment of more than 12 months. Foreign travel orders have a high statutory test, rely on open material and last for 6 months. Foreign travel orders have not yet been used (see paras 12 below re licence conditions).

11. The Royal Prerogative enables the Home Secretary to remove a British passport on public interest grounds. This does not prevent the travel of dual nationals or non British nationals residing in the UK. There are immigration options available for non British nationals. The government can deport non British nationals who are not conducive to the public good, exclude non British nationals on the basis of national

security or unacceptable behaviour, or deprive citizenship if not conducive to the public good or obtained by fraud.

12. Bail act conditions and licence conditions in relation to suspects and offenders can also be used to prevent travel. Convicted terrorists often have long licences which include restrictions on travel, hence the lack of foreign travel restriction orders. While there are clear options it is sensible to take stock and assess whether further legislation could assist. The police have been engaging with the Home Office and other partners to review existing powers and establish if they can be improved or amended.

13. Proposals for new legislation are being considered. Discussions resulted in inclusions in the Anti-Social Behaviour, Crime and Policing Bill 2013-14 currently before Parliament in relation to powers in support of the Royal Prerogative. Recently discussions have focused on whether TACT offences are sufficient and have the appropriate jurisdiction.

Overseas Capacity Building

Question 5. ***What role do the Metropolitan Police play in supporting the FCO's justice and human rights partnership programme? How does this work co-ordinate with the work of NCA officers - can you be sure that your work is not overlapping?***

14. The Metropolitan Police Counter Terrorism Command's (SO15) oversees a network of Counter Terrorism and Extremism Liaison Officers (CTELOs) and has recently expanded its geographical footprint in response to an expanding and more diversified threat overseas. It is now more effectively placed to deliver the policing component of our upstream counter-terrorism operations so that we can tackle the threat at its source and where there is a direct threat to the UK or its interests. The CTELO network plays a strong role in the Justice and Human Rights Partnership programmes (JHRP) in priority countries and we are supporting all of the seven currently active JHRP projects, including the CAPRI programme in Pakistan.

15. The nature of this support will vary depending on the context but has included training and mentoring local CT police units in evidence based investigations, interviewing and forensic techniques, where we place a heavy weighting on the importance of human rights compliant processes and safeguards to deliver reliable and viable prosecutions. The CTELOs work closely with their FCO and CPS colleagues and coordinate with other foreign partners to deliver their objectives. The CT Policing Network provides human rights compliant capability training to overseas partners.

16. CTELOs regularly liaise with NCA colleagues where we have common posts, although our operational focus is often different and, in many instances, our interaction will be with different foreign and UK partners. That notwithstanding, the CT Network is actively engaged with the NCA in examining potential areas of coordination and collaboration and some of these overlaps may well be identified in capacity building activity, specifically where we are interacting with the same organizations overseas. The NCA chairs a regular international coordination group meeting where these areas of common interest can be examined. Taking advantage of the ability to coordinate our

efforts with the NCA and other law enforcement agencies such as the AFP and FBI is central to our operating ethos.

Question 6. ***What was the scale of Metropolitan Police involvement following the In Amenas and Westgate terrorist attacks?***

17. The events at In Amenas and Westgate illustrate the very practical response that UK CT policing is able to deliver in crisis situations involving UK interests and citizens overseas. The In Amenas attack resulted in a deployment of a team of CT police forensic experts and investigators. They initiated and led negotiations on establishing multi-national partnerships to put in place victim identification and evidential forensic recovery processes in support of the UK Coronial investigation. In the UK and elsewhere, the SO15 established reception points at airports for witnesses to give evidential accounts of the incident, worked within the FCO and BP crisis and control centres to coordinate operational response and family liaison issues. The engagement with the victim's families continues alongside supporting the Coroner's inquest process.

18. SO15 has made a significant investment in mentoring and training the Kenyan Anti-Terrorist Police Unit (ATPU) through the two Counter Terrorism and Extremism Liaison Officers in Nairobi. This work is in support of the Justice and Human Rights Partnership project in Kenya. During the Westgate Shopping Centre attack, the CTELOs advised on implementing critical incident management and command & control processes in anticipation of the incident moving from military to police control. The ATPU operation was managed from the UK built ATPU operation centre, which provided an intelligence fusion centre again mentored by the CTELO. Critical CTELO support was maintained throughout the incident and was supplemented by the deployment of a police Disaster Victim Identification (DVI) forensic team - consisting of 10 officers - to work with the Kenyan police on the forensic examination of the scene and identification and examination of victim's remains to international standards.

Operation Spade

Question 7. Whether the Metropolitan Police received the names of Britons suspected of child pornography offences sent by the Canadian Police to CEOP 18 months ago as a result of Operation Spade and if so, what was done with the information?

19. The Metropolitan Police Sexual Offences, Exploitation & Child Abuse Command received an initial referral from CEOP on 26 November 2013 regarding Operation Spade. Full material was supplied on 29 November and an initial assessment was then conducted of this material. *Operation Eiger* was established to manage the MPS response and that operation continues.

Female Genital Mutilation

Question 8. Statistics regarding the number of victims who have come forward and the number of referrals from secondary witnesses

20. The total number of cases reported to the MPS since Project Azure commenced in January 2010 is **159**. Of those, the number of direct to Police referrals is **41 (25.79%)**. The remainder are **118 (74.21%)** secondary witness referrals.

Anonymised details of cases where the Metropolitan Police have investigated Female Genital Mutilation.

Each of the **159** referrals that have been made has been subject to investigation and safeguarding outcomes as appropriate. There have been **ten** cases referred to the CPS, four of which are still under review.

There are a number of barriers to prosecution of FGM, which will be fully explored in the MPS response to the committee. One of these barriers is the reluctance of those concerned to report to police. Cases of FGM relate predominantly to juvenile victims and it would be wholly inappropriate for the MPS to divulge details of individual cases. Given the small number of referrals to police it is not possible to provide meaningful anonymised data regarding individual cases without the potential for compromising victim confidentiality.

In order to assist the committee without compromising the trust of the victims, the key themes identified are highlighted below.

- Difficulties in prosecuting otherwise caring family members without the support of the victim

- Legal limitation of the FGM Act 2003 preventing prosecution where the victim is not a UK national

Alison Duncan-Mercy
Head, ACSO's Strategic Briefing Unit
February 2014

Supplementary written evidence submitted by Guardian Media Group [CT 25]

Letter from Alan Rusbridger, Editor-in-chief, Guardian News & Media, to the Chair of the Committee, 3 March 2014

Thank you for your letter of 27th January asking for the Guardian's views on the functioning of the DA Notice Committee.

In recent months there has been confusion within Government about the role and status of the DA Notice Committee1[1]. Indeed, the minutes of the 7th November meeting of the Defence, Press and Broadcasting Advisory Committee (DPBAC) detail how the Secretary of the Committee responded to the Prime Minister's statement of 28th October by "explaining the nature of the DA notice System"[2]. Those minutes also suggest that understanding of DA Notice operations have not been helped by absence from meetings by key government officials.[3]

As the Committee will be aware, the DA Notice committee is entirely voluntary and has no legal authority. The Committee comprises senior representatives from the Home Office, Foreign Office, Cabinet Office, UK Defence forces and the media.

Even after dialogue with the Committee has taken place, the decision as to whether to publish a given story, lies solely with the editor or publisher of that story. The interactions between the DA Notice and publishers are, in theory, confidential in nature. However, as I made clear to this Committee when giving oral evidence last year, the Guardian is concerned that confidential conversations about particularly sensitive stories may be a prelude to injunctions and other forms of prior restraint by Government in the name of a vague and broad ranging notion of national security. Such concerns are evidenced by historic interventions such as the 1987 injunction against the BBC4[4], and by the Cabinet Secretary's more recent threat to the Guardian that such restraint may be imposed.

Given the wide terrain across which the intelligence agencies now operate, and the broad legal framework within which they work, the Guardian is extremely concerned about attempts to strengthen the use of prior restraint by Government to prevent the debate of difficult, sometimes embarrassing issues, which are nevertheless in the public interest.

As I stated to this Committee in evidence last year, the idea of a body that exists to impose prior restraint on the media is a complete anathema to a United States audience in a post Pentagon Papers world. By contrast in the UK, the Guardian is concerned that the potential aim of reform of the DA Notice Committee may be to put prior restraint on a more formal footing.

To some of its critics, the DA Committee represents the worst of British institutional power dressed up as informality. On the other hand, colleagues have found the Committee's advice and dialogue throughout the vast majority of reporting of the Snowden files useful and constructive.

The DA Committee is imperfect in many ways. However, it is a peculiarly British solution to the difficult problem of ensuring that reporting in the public interest takes account of concerns about the national interest, without stymieing debate.

1 http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131028/debtext/131028-0001.htm#131028-0001.htm_spmin37

2 http://www. Ibid dnotice.org.uk/records.htm

3 Ibid

4 See for example, Secrecy and the Media: The Official History of the United Kingdom's D-Notice, By Nicholas John Wilkinson, Page 422 onwards

Any replacement for the body would therefore have to demonstrate to the public and to the media, that it struck that balance in a more effective way, or risk further undermining the right of journalistic free expression, and reinforcing the increasingly widespread view of a UK Government clampdown on the right to free and independent press.

I enclose with this letter a short note which provides specific observations in relation to our experience throughout reporting of the Snowden files, and some brief thoughts on potential areas for reform.

I do hope this covers the points raised in your letter.

Alan Rusbridger
Editor-in-chief
Guardian News & Media

Annex

Observations in relation to the reporting of the Snowden files

1. The DA Notice system serves a useful function in two main ways

> a. It serves as a forum where defence, intelligence and media people can meet and discuss things;
> b. It can be a valuable way of checking sensitive matters in advance so as not inadvertently to risk national security or operations. We have had repeated contacts with the officials in the last six months or so, and have found them helpful, trustworthy and – so far as one can tell – independent.

2. Since the Snowden story began in June 2013, the Guardian has found it generally easier to have a direct dialogue with the American intelligence services and government than in the UK.

3. The Snowden files contain often highly technical and complex material, of which, even long term agency staff don't necessarily have a detailed grasp. As such, our experience has been that conversations between editors, highly specialist reporters and 'subject specialists' at the agencies have been more effective at assessing whether to withhold or redact material than going through a middle man process such as a DA Notice model. In the UK, there is a sense in which the DA Notice system replaces good direct communications between the services and journalists.

4. For the system to work there has to be trust that:

> a. there are true Chinese walls between the DA Notice officials and the intelligence services;
> b. an approach to the DA Notice officials will not trigger pre-emptive action by government or its lawyers;
> c. the officials will make independent judgements about the agreed criteria and not be “leaned on” by the government or agencies.

5. The system must also be advisory and not binding. The ultimate judgements must be made by editors. One example related to Snowden: we received advice from the DA Notice officials not to run a story about the extent to which the NSA had undermine the security of the web itself. Yet many people – including international journals, academics, businessmen, legal scholars and technologists – believed this was the most important story of all.

6. The legal regime in the UK – with the ever present threat of prior restraint (explicitly made in the Snowden case) – contrasts with the situation in the US, where the first amendment is

reinforced by the Supreme Court judgement in the Pentagon Papers case. It is virtually inconceivable that the US Government would have attempted – far less succeeded – the gagging the NYT or Washington Post over their Snowden coverage. The NSA's general counsel went further in debate over the autumn when he said that – while the agencies and government deplored the Snowden leak – once the material was in the hands of a newspaper, the journalists were protected.

7. In the UK – where judges have shown themselves quite ready to grant injunctions preventing publication – it is harder to engage in full and frank discussions with the authorities. Our colleagues in America found it more natural to have advanced conversations with the US intelligence services, knowing that there would be no attempt to frustrate publication.

8. Once the UK Government effectively forced the Guardian's reporting out of the jurisdiction it lost a degree of influence over the reporting. Our reporting was done in collaboration with ProPublica and the NYT. On more than one occasion we placed a higher value on the contacts between the NYT and White House than any parallel conversations with the UK government. By seeking short term control over the Guardian, the Government lost long term influence.

9. It is not clear that the DA Notice mechanism, the agencies or the government have fully grasped the complexities of the new media environment. The more restrictive they are towards mainstream media, the greater the likelihood that future leakers or whistleblowers will bypass traditional organisations and publish through channels which they regard as "freer" – or even publish directly to the web themselves.

10. We therefore urge against knee jerk instincts to discard the valuable mechanisms which do enable some form of communication over the handling of sensitive material particularly given that the government and intelligence agencies have shown limited appetite for true engagement.

11. We hope that the Snowden reporting could stimulate a constructive dialogue between media, government and agencies about how to modernize the relationship between them. We hope this discussion might include a consideration of moving the Government's attitude towards prior restraint to be more in line with that which exists in the US.

Suggested amendments to the DA notice system

12. Suggested amendments to the operation of the DA Notice system have historically followed disagreements between the Government of the day and the press about whether a specific story should have been published.

13. Calls in 1967, by the Wilson Government, for reform of the DA Notice system followed a Daily Express story entitled '*Cable Vetting Sensation'* which outlined how the Government of the day was vetting private communications flowing across cable networks. Ultimately, Wilson's calls for reform were opposed, not just by the media, but also by a Committee of Privy Councillors whom he directed to investigate the matter.

14. Similarly in 1987, the system was called into question after the government sought an injunction against BBC Radio 4 for the programme 'My Country: Right or Wrong'. The injunction resulted despite the BBC following the appropriate procedures, and being confident the programme did not endanger national security. The confidentiality of the process was brought into question when the Attorney-General, who apparently learnt about the number of former security service personnel taking part in the programme from a newspaper gossip column, obtained an injunction against the programme.

15. As outlined in the cover letter to this note, the DA Notice Committee is by no means a perfect solution. However, in the absence of any compelling alternative proposals for wholesale reform, the Home Affairs Select Committee may instead look at a number of reforms and tweaks to the DA Notice Committee which could include:

a. **Direct representation of national newspapers on the Committee.** There are currently no newspapers directly represented on the DA Notice Committee. Representation is instead through the NPA and NS. It may benefit the Committee to have direct representatives of newspapers within its midst;

b. **A review of the guidelines by which the Committee recommends that stories should not be published**. This review should be conducted in consultation with the media, with the aim of better reflecting both the changing nature of: surveillance; of the media; and of the digital distribution of information;

c. **Learning from the US system of constructive discussion between the White House, agencies and publishers**. Perhaps because the Americans are the senior partner in the NSA/GCHQ relationship, they feel more able to recognise elements of stories that are genuinely of concern, and those which are merely embarrassing. There may however, be elements of best practice about direct communication between the agencies and the press that the DA Notice Committee could adopt from the US model.

Guardian Media Group

February 2014

Written evidence submitted by Claystone Associates [CT 26]

Claystone Associates is a non-profit civil rights advocacy group. Claystone conducts research, provides consultation services and campaign development to foster social cohesion in relation to Muslims in British public life.

Our submission to the inquiry offers both a broader view of how counter terrorism measures are often perceived as well as some specific concerns as to how they are manifesting themselves and thereby impacting civil society.

Has counter terrorism gone too far?

Even though the expression 'War on Terror' might not be used by politicians as much now as it has been in the past, the legacy of the 'War on Terror' is embedded in legislations, institutions and practices across the globe. In some research by Prof. Jude Howell, Centre of Civil Society and Dr Jeremy Lind, University of Sussex, they consider it possible to conceive the 'War on Terror' as a regime, characterised by a complex weaving of discourses, political alliances, policy and legislative shifts, institutional arrangements and practices.[1]

The key features of this regime are that it has:

1. served as a mobilising discourse that politicians and leaders have used to justify their political, geostrategic and military objectives;

2. used militaristic language and rationalised extraordinary responses such as pre-emptive military intervention;

3. provided a polarised vision of the world that pits barbarism against civilisation, modernity against backwardness, good against evil, freedom against oppression;

4. led to a global political re-ordering with a new set of institutional and policy arrangements.

The theory of the radicalisation conveyor belt

5. Counter Terrorism prevention is largely built on the assumption that there is a radicalisation process that acts like a conveyor belt. It is claimed that non-violent extremism leads to violent extremism. This link is tenuous and un-evidenced. One could equally make the claim that it is in fact perceived violent injustice which is resulting in violent retributive injustice. Unsurprisingly the latter is not a much considered narrative since for any government to acknowledge this would mean accepting that they are at the very least an actor in the process, thereby leaving room for potential culpability.

[1] http://www.lse.ac.uk/internationalDevelopment/research/NGPA/publications/Counter-terrorism%20and%20civil%20society%20final%20version.pdf

6. CIA officer Marc Sageman, who also advised the New York Police Department and testified in front of the 9/11 Commission, described the conveyor belt theory as "nonsense" and says there is little empirical evidence for such a 'conveyor belt' process. "It is the same nonsense that led governments a hundred years ago to claim that left-wing political protests led to violent anarchy."[2]

7. There were media reports in December 2013 that the government holds a list of 25[3] extremist speakers that have broken no laws, yet the government intend to serve behaviour orders for extremism to stop them speaking publically. Following this Claystone asked the Home office in a freedom of information request if there is in existence a list of public speakers who are considered to preach extremism or intolerance? We also wished to know the criteria for being placed on the list or indeed being removed from the list. Their official response was troubling as they would neither confirm nor deny its existence.[4]

Claimed issue of radicalisation and by non-violent extremism on university campuses

8. Both the media and the government have made assertions that radicalisation is occurring at universities. This claim was challenged by the representative body for UK universities, Universities UK, in its 2011 report 'Freedom of speech on campus: rights and responsibilities".[5]

9. Universities UK Chief Executive, Nicola Dandridge, suggested that universities had no more of a problem [with respect to violent extremism] than the rest of society and stated that students had to be left to monitor visiting speakers themselves. In addition to this, Ms Dandridge stated that she had obtained advice from the police and MI5: "They are telling us that there is not necessarily a link that they can prove between open debate in universities and violent extremism subsequently."[6]

10. Ms Dandridge the chief executive of Universities UK said universities had been unfairly singled out for attention, because many terrorists went to university, "but they tend to be young people and 40 per cent of young people go to university."[7]

11. This is a view shared by the National Union of Students (NUS) whose then President, Aaron Porter, suggested it was "…irresponsible of Theresa May to try to shift the blame for non-violent extremism onto universities or students." He further added:

[2] http://www.huffingtonpost.co.uk/2013/05/27/sageman-interview_n_3342206.html

[3] http://www.thesundaytimes.co.uk/sto/news/uk_news/National/article1355803.ece

[4] https://www.whatdotheyknow.com/request/193507/response/492898/attach/html/3/attachment.pdf.html

[5] http://www.universitiesuk.ac.uk/highereducation/Documents/2011/FreedomOfSpeechOnCampus.pdf

[6] http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8542599/Universities-have-no-problem-with-radicalisation-chief-claims.html

[7] *Ibid.*

"Facing up to the challenges that non-violent extremism brings to campus life requires careful support and guidance from Government, not wild sensationalism that only serves to unfairly demonise Muslim students."[8]

12. Claystone conducted an exploratory report investigating incidents wherein universities cancelled Islamic society events that were to host visiting speakers.

13. These cancellations took place without the consent of the Islamic societies. The reasons for these cancellations, as identified by the study, were primarily due to:

i. Pressure placed on the universities from external groups

ii. Universities claiming that the visiting speakers promoted views that were not consistent with its values[9]

14. Our study found that universities were acting to cancel events without verifying allegations provided by pressure groups against speakers. This had resulted in reversals to decisions of banning speakers later taking place. It also meant Islamic societies encountered unnecessary obstacles to their activities and may have restricted freedom of expression on campus.[10]

15. The main pressure group involved is a group called 'Student Rights'. Despite their name they are not run by students nor do they have any student membership. Hiliary Aked a researcher at the University of Bath has suggested they are a front group for the Henry Jackson Society neoconservative think tank.[11]

16. An article in the Times newspaper states "Regarding the Henry Jackson Society – to whose principles David Willetts, the universities and science minister, is a signatory – he said that Student Rights was "a project of" the think tank and shared an office with it, but it raised funding independently."[12]

17. Such revelations give cause for concern that issues are being contrived to give credence to pre-conceived problems that facilitate particular narratives.

[8] http://www.theguardian.com/education/2011/jun/06/theresa-may-extremism-university-islamists

[9] http://www.claystone.org.uk/wp-content/uploads/2014/02/Claystone_AccessDenied.pdf

[10] *Ibid.*

[11] http://www.huffingtonpost.co.uk/hilary-aked/student-rights-campaign_b_4452823.html

[12] http://www.timeshighereducation.co.uk/news/students-unions-hit-back-at-group-monitoring-campus-extremism/2010074.article

The Charities Commission

18. As part of counter terrorism measures it has been asserted that the charities commission plays a vital role in cutting off potential funding to terrorist organisations. Resulting from this presumed relationship between charity abuse and terrorists is the belief that the response of the charities commission will serve as a critical component to tackling the financing of terrorist related activities.

19. It is our belief that funding for terrorism through the abuse of charity status is an over-stated concern. This has been acknowledged by David Walker who in 2009 was head of outreach, compliance and development in the compliance division of the charities commission. On 6th March 2009 in a lecture said 'Our assessment as a regulator is that terrorist abuse is actually very rare in charities'[13]

20. In a study by Prof. Jude Howell, Centre of Civil Society and Dr Jeremy Lind, University of Sussex, an interviewee from the charities commission said: "Our approach is more light touch regulation that will be effective, which does not overburden the sector. It is a risk based approach and our approach is miles away from the sledgehammer approach in the US, where if there is doubt, you just take out the charity"[14]

21. We believe that evidence already submitted to the committee asserting that The U.S. Treasury has designated Interpal as a terrorist organisation in 2003 needs to be seen in light of the above.

22. There is concern that the remit of the charities commission seems to have widened from concern about charities funding terrorism to charities giving a platform to those deemed proselytizing an extremist ideology that leads to radicalisation then possibly to terrorism.

23. Governments have consistently failed to substantiate claims that charities are misused by terrorist networks. Under the Bush administration, Dick Cheney said: "If there is a *"if there is a 1% chance that Pakistani scientists are helping Al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response, it is not about our analysis, it is about our response"*. [15]

24. We feel it is important for the government to step back and look at how the tentacles of counter terrorism policy seem to be spreading deeper and wider than ever conceived at its inception. It is our belief that the adoption of the 1% doctrine is 100% dangerous for us to maintain a free society.

Claystone Associates
March 2014

[13] http://www.lse.ac.uk/internationalDevelopment/research/NGPA/publications/Counter-terrorism%20and%20civil%20society%20final%20version.pdf

[14] *Ibid.*
[15] *Ibid.*

Supplementary written evidence submitted by
Gilles de Kerchove, EU Counter-Terrorism Coordinator [CT 27]

Subject: Response to request for information by the Home Affairs Committee

Following my appearance before the Home Affairs Select Committee on Tuesday 28 January, you sent me a letter requesting additional information on the subjects we discussed during the hearing. With this letter, I am happy to respond to your requests for information on specifically foreign fighters and overseas capacity building.

Foreign Fighters

• What can be done to reduce the threat that foreign fighters pose to their home nations? Does there need to be more co-ordination on this issue between member states? Please give us examples of where EU member states have responded well to this threat.

It is clear that only a comprehensive response will help to mitigate the threat. Work is needed in different areas at the same time, both by the EU and its Member States. The bulk of the response is internal, and responsibility lies with Member States. There are nevertheless four areas where EU action in support of Member States' efforts would be particularly important:

- Dissuading individuals from traveling to Syria to fight through 1. improved communication and messaging initiatives regarding Syria both within the EU and in third countries, 2. Targeted efforts to counteract more effectively the use of the Internet and social media for radicalisation and recruitment purposes, and 3. given some of the individual's understandable desire to help the people of Syria, diverting their energies towards non-violent and more positive outlets, e.g. humanitarian support.
- Identify and detect individual foreign fighters when they travel to Syria, and when they return to their country of origin and/or other countries through a better use of existing EU instruments for information exchange (Schengen Information System, establishment of PNR, Entry/Exit)
- Develop an effective criminal justice response to the phenomenon of foreign fighters through increased cooperation with Eurojust, Europol and Frontex.
- Step up cooperation with third countries through focused political engagement and continued dialogue, increased information exchange, operational cooperation and – crucially – capacity building.

There already seems to be a strong co-ordination on this issue between member states. The competent Ministers of the most concerned Member States have met several times in the margins of the Council. Also the services seem to exchange well. Most exchange of information, however, still seems to happen on a bilateral basis, but given the cross border nature of the phenomenon, it is also important that Member States' services share information on a multilateral level. It is not inconceivable that a foreign fighter could return to his home country with the intention of joining former comrades for an attack in another. Hence, information needs to be shared appropriately and quickly.

There are numerous examples of where EU member states are trying to develop the most adequate responses to this threat. Some EU Member States have set up multi-disciplinary platforms to deal with returnees and to decide on a case-by-case basis which kind of intervention and support is most appropriate. Others have looked into administrative

sanctions particularly to prevent or disrupt travel to Syria. The UK has developed one of the best communication campaigns, which not only raises awareness of the phenomenon and the possible risks related to it, but also offers an alternative to those who want to go to Syria for humanitarian reasons.

• What is the European Council doing to address this threat?

The Council had several in depth discussion on the issue of foreign fighters and returnees from a counter-terrorism perspective, in particular with regard to Syria, on the basis of a number of documents prepared by the EU Counter Terrorism Coordinator (CTC), in close consultation with the Commission and the EEAS.

In February/March 2013, the implications of Sahel / Maghreb (crisis in Mali, IN AMENAS) on EU internal security[1] were extensively debated at COSI/PSC and the Council. Among other issues to be followed up, the CTC was requested to take work forward on foreign fighters in particular.

In May 2013, the CTC presented an initial paper entitled "Foreign fighters and returnees from a counter-terrorism perspective, in particular with regard to Syria"[2] to COSI/PSC, setting out a comprehensive analysis of the various aspects of the phenomenon and a number of suggestions for possible measures to be taken. Following this discussion, the CTC issued a second paper[3], which listed 22 recommendations and priorities for action. Recommendations were made in the following clusters of issues:

- the need for a common assessment of the phenomenon of young Europeans going to Syria for Jihad and the need to obtain a better picture of the different groups fighting in Syria;
- measures to prevent youngsters from going to Syria or to offer assistance on their return;
- detection of travel movements and the criminal justice response;
- co-operation with third countries.

The Council broadly endorsed the recommendations and asked the CTC to present a report[4] on their implementation to a joint meeting of COSI/PSC in November, in preparation for a follow-up discussion at the December JHA Council.

In December 2013, the Council endorsed the CTC's stocktaking paper[5] that identified four priority areas where EU action in support of Member States' efforts would be important. These four areas were described under the first bullet point above.

• Is this a priority of the European External Action Service?

The EEAS has stepped up its engagement on this issue over the past few months.

[1] 6983/13, 6752/13
[2] 9036/13
[3] 9946/13
[4] 15955/13
[5] 16768/13

Foreign Fighters are now raised in all EU CT dialogues with third countries, and in all appropriate high-level contacts.

The EEAS has established an inter-institutional working group to co-ordinate on Syria Foreign Fighters. Following discussion at PSC-COSI in November (noted above), and a non-paper outlining proposed third country action, the EEAS has agreed with the CTC and Commission a plan for strategic engagement with third countries. The EEAS, along with the CTC's Office, is now working to put this plan in to effect, and identify concrete measures that can be taken to address the threat upstream – such as capacity-building in priority countries - before it manifests itself in our home countries.

• How many bank accounts were frozen under EU regulation 2580/2001 in 2013? Is this tool being used against those who are fighting in Syria and if not, why not?

As far as I am aware, no bank accounts have been frozen under regulation 2580/2001 in 2013.

Overseas Capacity Building

• The EU has set up a number of programmes where it works to build capacity and ensure that responses to terrorist activity are in line with the rule of law. Please give us details of some of the projects that are currently running?

This has been a major focus of EU's external CT-related work. For example, under the Instrument for Stability long term, the instrument with a specific CT allocation:

CAERT: 585,000€, 36 months (01/10 – 01/13), African Union (AU). The objective was to support the fight against terrorism in the African Union by strengthening the African Centre for Studies and Research on Terrorism (ACSRT – or CAERT in FR) and the AU focal points structure.

Global Outreach: 2,000,000€, 24 months (05/2012 – 04/2014), Cambodia, Indonesia, Lao PDR, the Philippines and Vietnam. The objective of the programme is to contribute to global security through supporting regional and national capacity in Southeast Asia to: (a) counter terrorism while fully respecting human rights; and (b) undertake related regional cooperation.

CT Sahel: 8,696,750€, 36 months (10/2011 – 10/2014), Mali, Mauritania and Niger, with possible extensions to Burkina Faso and Senegal. The aim of the project is to strengthen the capacities of law enforcement (police, gendarmerie and garde nationale) and judiciary in the Sahel to fight against terrorism and organised crime with the purpose to support the progressive development of regional and international cooperation against these threats.

CT Pakistan (CAPRI): 1,800,000€, 36 months (01/2013 – 12/2015). The overall objective is to support national capacity in the fight against terrorism and organised crime networks. The purpose of the action is to improve the ability of Punjabi agencies to successfully investigate, prosecute, convict and detain terrorists. The project is being carried out by the UK.

STRIVE Pakistan: A 5 M€ project on countering violent extremism and radicalisation has been prepared for implementation starting in 2014. The specific objective is to reinforce

Government, media and civil society capacities in Pakistan to countering violent radicalization at provincial and federal level.

STRIVE HoA: A 2 M€ project aims to develop best practices for countering violent extremism and radicalisation in the Horn of Africa and Yemen. Concretely, the aim is to constitute a knowledge base on past and present practices with recommendations for evidence based policymaking and action planning. The project was prepared in 2013 and will start implementation in January 2014.

CVE Training Workshops: To improve the capabilities of EU staff of developing CVE specific interventions using existing and future development efforts to contribute to the prevention of violent extremism and terrorism a series of thematic trainings on CVE are in the process of being prepared to be conducted in Africa and Asia. The first training was conducted in Kenya in December 2013 with the remaining workshops scheduled for the first part of 2014.

CFT HoA: A 6 M€ project related to Countering the Financing of Terrorism (CFT) cooperation in the Horn of Africa and Yemen was developed with implementation from early 2014. The specific objective is to contribute to the national and regional capacity to meet international standards on effective anti-money laundering and counter-terrorist financing in the sub region, through capacity building and networking.

A 3 M € project under the European Neighbourhood policy instrument "Supporting rule-of-law compliant investigations and prosecutions in the Maghreb region" carried out by UNODC and UNCTED and implementing the EU's Maghreb Communication will run from 2014-207. The objectives are to increase the capacity of criminal justice and law enforcement officials to effectively investigate, prosecute and adjudicate terrorism cases in the Maghreb, in line with the relevant international legal instruments and Security Council resolutions; to strengthen the capacity of selected Maghreb countries to apply human rights norms, standards and good practices in counter-terrorism measures, and to assist them achieve human rights compliance in their criminal justice responses to terrorism.

- What budget does the EU have for Counter-terrorism work?

The long-term component of the Instrument for Stability – now renamed the Instrument contributing to Stability and Peace – is the only instrument which has specific allocation for external counter-terrorism. The annual allocations are still be calculated, but will average around €18m per year.

The new Internal Security Fund might also be used in the future.

However, there are a range of other instruments that can be used to support CT-relevant work abroad. For example, the IcSP crisis response mechanism, as well as the European Neighbourhood Programme, have both funded external CT work. These instruments do not, though, have a specific allocation for external counter-terrorism.

In addition, the regular development cooperation instruments such as the Development Cooperation Instrument or the European Development Fund can be mobilized to fund projects on prevention of radicalization, on strengthening the law enforcement and criminal justice response to security threats and to provide security sector reform. Therefore,

recognizing that terrorism is increasingly an obstacle to development, in particular in Africa, it is important to fully realize the opportunities that the OECD/DAC provides (for example: DAC reference document: A Development Cooperation Lens on Terrorism Prevention - Key entry points for action).

Upon request of interested partner countries, EU instruments such as TAIEX (to organize workshops and provide short term expertise) and longer twinnings can be used in the candidate countries and countries benefiting from the EU's neighbourhood policy to provide assistance and share expertise on CT. For example, a successful twinning was carried out to assist a country in North Africa in the establishment of its Financial Intelligence Unit. These instruments require EU funding and Member States' expertise.

EUCAP Niger is the first EU CSDP operation which is providing CT capacity building assistance.

In the past, CFSP funding has been used for CT projects, this could be done again.

CEPOL, the European Police College, has started to engage in training of police of partner countries. This could be broadened to include CT.

- How are you planning to measure the effectiveness of these projects?

Before a project is started, assessments are carried out at political and technical level. An overview of other donor's activities is established, to find the right gaps.

The EU has only very recently started to engage in CT projects, therefore most of the projects, which took some time to set up, are still running. There was a comprehensive mid-term review of the CT Sahel project, carried out by outside experts, which assessed the effectiveness of the project so far and made useful recommendations for the way forward.

Projects are subject to monitoring and adjustment throughout their life, as well as assessments and review at their closing.

The more CT projects the EU engages in, the more relevant the incorporation of lessons learnt for the future will be.

However, it continues to be a challenge to assess the effectiveness of preventative work. A recently-launched project in the Horn of Africa, entitled Strengthening Resilience against Violence and Extremism (STRIVE), aims to act as a pilot in this regard and identify best practice which can be applied to similar work elsewhere.

- How can the EU ensure that member states are co-ordinating their overseas capacity building efforts and that they are not running similar projects in the same places?

Counter Terrorism is to a large extent a Member State competence. Part of the key added-value of EU engagement is to ensure that Member States are co-ordinating overseas capacity-building. We therefore lead donor co-ordination in various countries around the world, as well as ensuring that we brief – and are briefed by – Member States through the relevant Council working groups. The EU carries out regular stocktaking to map existing projects, in particular before deciding to embark on additional (complementary) initiatives. In addition,

the Global CT Forum (GCTF) should gradually play a role in ensuring co-ordination and consistency of effort.

• Are there enough resources being placed in capacity building or should we be investing more?

National budgets devoted to counter-terrorism are declining, across the EU. Yet the threat that we face is becoming more diverse, more diffuse, and more unpredictable. In particular in Africa, the terrorism threat is growing and becoming a major obstacle to development. The risk posed by returning Syria Foreign Fighters is unprecedented, and all the reports I have seen suggest that it is becoming increasingly acute. Mitigation will require concerted and co-ordinated action internally, as well as action externally – addressing the threat to avoid de-stabilization of the partner countries and the establishment of terrorist safe havens. This is about the security of the partner countries and our own security.

We should be investing a lot more in counter-terrorism work, including externally, if we are to prevent or mitigate future terrorist attacks. It will be crucial to use the available EU financial instruments and for Member States to mobilize expertise to carry out the projects.

A focus purely on CT specific projects will not be enough: A comprehensive security and development approach is needed, such as in the EU's Sahel Strategy. It is crucial to create jobs and educational opportunities to provide viable alternatives to youngsters. Rule of law and human rights compliant security, law enforcement and criminal justice systems need to be strengthened generally, this will also provide a better basis for CT work.

The EU's agencies CEPOL, Europol and Eurojust should be encouraged to invest more in the relations with third countries on CT.

I hope this information sufficiently answers your questions.

Yours sincerely,

Gilles de Kerchove, EU Counter-Terrorism Coordinator

March 2014

Supplementary written evidence submitted by Jean-Paul Laborde, Executive Director, UN Counter-Terrorism Committee Executive Directorate [CT 28]

Response to questions posed by Home Affairs Select Committee on Counter-Terrorism

Why are capacity-building projects important?

- The promotion of international cooperation, as enshrined in the international legal instruments of the United Nations, is essential to achieving national and international security. The transfer of know-how, through capacity-building programmes, and technical assistance and training on identified areas of need, from high capacity countries to lower capacity countries, and through the activities of multilateral agencies, such as those of the United Nations, not only builds capacity where required, but also identifies best practices, and creates regional and international networks of specialists and fosters the habits of cooperation at the working level.

How can the effectiveness of capacity building projects be measured?

- By conducting analysis of national implementation of Security Council resolution 1373 (2001), which the Counter-Terrorism Committee of the Security Council has been undertaking since 2002, in conjunction with accurate and timely record-keeping and analysis of the capacity building projects provided by multilateral and bilateral partners. CTED undertakes this work in collaboration with its partners within and outside the UN system. It works with them to develop the appropriate tools and methodologies to measure the impact of the work that CTED and its partners are undertaking in order to ensure that counter-terrorism measures are effectively deployed.

Is there enough co-ordination in terms of capacity building in countries which are considered to be at risk from terrorist activity?

- Coordination of capacity-building is an ongoing undertaking for multilateral and bilateral donors and providers of technical assistance. The United Nations plays a central role in this and CTED, in particular, undertakes several activities to ensure coordination of delivery of capacity building to avoid duplication. They involve intensive work with other multilateral organizations, including UN agencies, and as mandated by the Counter-Terrorism Committee, including through joint participation of several international and regional organizations in on-site visits to at-risk States, the regular convening of donors and providers for briefings on capacity-building needs in particular States or regions, the regular convening of recipient States in fora designed to understand their needs, and the active

collaboration of groups of multilateral and bilateral donors and providers in organizing coordination meetings and outreach to recipient States that are at risk from terrorist activity, as well as general information-sharing. Within the United Nations, CTED regularly briefs and is briefed by other agencies, which ensures that the UN speaks with one voice and delivers a consistent message on counter-terrorism, rule of law and the protection of human rights.

Are there adequate resources made available for capacity building programmes?

- There are never enough resources available to do all the work that the United Nations and CTED, in particular, are tasked to do. This is understandable in the current financial climate, since all States have had to make cut-backs in their own expenditure. However, CTED, like its partners, works hard to "do more with less" by developing capacity-building projects that are designed in very practical ways to maximize the use of resources. These include the implementation of regional approaches, in which capacity-building addresses the needs of a number of countries at once. This has the added advantage of enhancing regional cooperation by promoting networks of officials across the region with similar skill-sets. Similarly, donors and providers frequently pool resources to collaborate on the deliver of capacity-building, particularly on larger projects – this, of course, has the additional benefit of enhancing coordination of capacity-building. CTED also works to build projects that facilitate further "spin-off" technical assistance and training by other donors and providers.

- An example of this would be the implementation of the ongoing CTED global project designed to develop effective and proportionate strategies to prevent terrorism financing through non-profit organizations (NPOs). This project, launched in London in 2011 with the support of the Government of the United Kingdom, was supported mainly by Canada and also by Australia, New Zealand, Sweden, Switzerland, the United Kingdom and the United States. The project brought together more than 60 countries and more than 80 NPOs to examine the risks. Experts from the United Kingdom, including the Charity Commission of England and Wales, played a leading role in the organization and implementation of this unique initiative, providing invaluable guidance and policy advice.

Jean-Paul Laborde, Executive Director
UN Counter-Terrorism Committee Executive Directorate
March 2014

Written evidence submitted by
Sir Mark Waller, Intelligence Services Commissioner [CT 29]

In response to your summons dated 25 February 2014, I would just like to explain why I have felt a reluctance to come and give oral evidence. The reason flows from my position as set out in the legislation and the sensitivity of the subject matter with which I deal. Under Section 60 of the Regulation of Investigatory Powers Act 2000 (RIPA) I must make an Annual Report to the Prime Minister who must lay that Report before Parliament. But under Section 60(5) the Prime Minster after consultation with me can exclude from my Report certain matters concerned with:-

(a) national security,
(b) the prevention or detection of serious crime,
(c) the economic well-being of the United Kingdom, or
(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by that Commissioner.

This has happened as a matter of practice introduced by my predecessors in a report being produced in two parts – open and closed.

I am sure your committee would accept that it cannot be right that, although by virtue of section 60(5) certain material on which I report cannot be revealed to Parliament, I could be forced to reveal such information by being asked questions by a select committee of Parliament. As I say I am sure that your committee would accept that but my anxiety relates to the fact that it is not always easy to explain why a matter is sensitive without revealing matters that should not be revealed and that can lead to misunderstanding and the impression of being unhelpful. The Intelligence and Security Committee of Parliament (ISC) do have experience of dealing with this type of problem and have access to all the material in my closed report which falls within their remit and that is why I have said that I would prefer to give evidence before that committee.

I remain of the opinion that the ISC is the appropriate place for parliamentary oversight but now that I have been ordered to appear before your committee I will do so and try and help as far as I can. I do ask the committee to bear the difficulties in mind.

It would help if the areas on which you would seek to ask questions could be clearly identified. In your previous letter you did identify some areas but introduced by the phrase “amongst other matters”. May I assume that you have identified the areas, if not could you please identify such other areas as you wish to cover.

Sir Mark Waller, Intelligence Services Commissioner
10 March 2014

Supplementary written evidence submitted by
Sir Mark Waller, Intelligence Services Commissioner [CT 30]

Inquiry into Counter-Terrorism

First may I thank you and the members of your Committee for your kind words at the conclusion of the session on 18th March and indeed for not seeking to go into sensitive areas during my evidence.

Can I however also seek to clarify certain points which came up during my evidence?

Firstly I believe I can provide follow up information regarding the number of warrants scrutinised in 2012. I provided the committee with the number I scrutinised at the intelligence services but I also scrutinise from the same list of warrants at the warrant issuing Government Departments. If one adds in these additional visits:

- in 2012 there were 2838 warrants issued
- during my oversight visits and reviews of the Government Departments in 2012 I scrutinised **242** or **8.5%.**

I will deal with 2013 in my Annual Report.

I should also make clear that I require the intelligence services and the warrant issuing Government Department to provide me with a list of all warrants issued, cancelled or lapsed since the previous list provided to me on which there is a summary as to what the warrant relates. I do thus in effect see in summary form every warrant and I am able to select any warrant from this list for further scrutiny. I hope that this provides you with greater reassurance.

I also indicated that I had reviewed the media allegations about the work of GCHQ with 18 months experience when, of course, by June 2012 I had 2 ½ years' experience.

In my report for 2013, I do expect to write more about these media allegations but I realise from the transcript that it appears I only saw the second in command at GCHQ to make my assessment. In fact I met with a number of senior officials who made themselves available to me including a GCHQ lawyer. I was also able to question Iain Lobban the head of GCHQ in order to come to the conclusion in my 2012 Report.

There are some figures which I said I would try to supply and I hope to do so in my 2013 Report.

Sir Mark Waller, Intelligence Services Commissioner
25 March 2014

Supplementary written evidence submitted by
Susan Cobb, Private Secretary, Intelligence Services Commissioner [CT 31]

Inquiry into Counter-Terrorism

Thank you for your letter dated 25 March 2014 requesting additional information from the Intelligence Services Commissioner regarding:

- The percentage of cases that the Commissioner looks at in which the consolidate guidance applies
- How many disciplinary proceedings were reported to the Commissioner in 2013.

Your request crossed with the Commissioner's follow up letter to Mr Vaz in which he says:

> "There are some figures which I said I would try to supply and I hope to do so in my 2013 Report."

As you know under s60 of the Regulation of Investigatory Powers Act 2000 (RIPA) the Commissioner must make an Annual Report to the Prime Minister who must lay that Report before Parliament. But under s60(5) the Prime Minster after consultation with Sir Mark can exclude from that Report certain matters concerned with:-

a) national security,
b) the prevention or detection of serious crime,
c) the economic well-being of the United Kingdom, or
d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by that Commissioner.

The statistics you have requested have not previously been made available to Parliament so I am currently in consultation with the relevant parts of Government to determine if the Prime Minister considers that the information requested can be laid before each House. It is with this in mind that the Commissioner said that he hoped to supply these figures in his 2013 Report.

Yours sincerely

Susan Cobb
Private Secretary
Intelligence Services Commissioner
25 March 2014

Written evidence submitted by Uthman Lateef [CT 32]

To whom it may concern,

I am writing this comment in relation to my inclusion in the Home Affairs Select Committee evidence found here http://www.parliament.uk/documents/commons-committees/home-affairs/CT%20Written%20Evidence.pdf

1) The following is from a personal response written last year: "The CSC (Centre for Social Cohesion) initially 7 years ago in 2007 sensationally defamed Dr. Lateef by misquoting the words “we abhor” – in the context of the irreligious act of homosexuality, and turning them into “we’re at war.” The audio recording is available and the deliberate misquote is clearly discernible and exposes CSC’s lack of professionalism not to mention its divisive approach. Upon being challenged on this sensational misquote the CSC then sought to build a case on a single statement pulled out of context. Dr. Lateef’s comment regarding homosexuality is one held by Muslims, Jews and Christians and only arose during a question and answer session, after specifically being asked about Islam’s view on homosexuality. At no time did Dr. Lateef insult anyone nor personalise his religious belief. Clearly, saying ‘we hate homosexuality” is not the same as saying “we hate homosexuals” which would be counter to the Islamic spirit and undoubtedly an offensive statement. Islam undeniably regards homosexuality to be a sin and something displeasing to God, and it was this that Dr. Lateef was stating, not that homosexuals should be hated, or vilified or ever abused.

Dr. Lateef is a well-respected speaker and academic who has been invited internationally to speak on a range of Islamic topics. He has received much acclaim from all portions of the community, Muslim and non-Muslim for his work on addressing social ills such as the knife crime epidemic among youth, child abuse and teenage suicides. (‘Shattered Dreams: The Dilemma of Childhood’; ‘Blade Britain and the i-empire’; ‘Envy Cuts its Own Throat’). Dr. Lateef is a khateeb at mosques throughout the country and speaks on issues that affect the wellbeing of all peoples. Recently, for example, after the killing of Lee Rigby, he publicly condemned the killing in the presence of around 2,000 worshippers."

2) Most recently, on Wednesday 26th 2014 I was invited to speak at Nottingham University by the Islamic Society at the university. The talk was entitled ‘The Paradigm of Justice’. The areas I focused on were realisation of each other’s humanity; constructs of Self and Other and how agitations are allayed through empathy; racism; discrimination and exploitations in our world. I spoke about human suffering and our empathetic responses. I spoke about domestic violence, child cruelty, child abuse. I spoke about neighbours’ rights. I centred my talk on overcoming the impediment of hate that disallows justice being realised, established in the Qur’anic verse: ‘O you who have attained to faith! Be ever steadfast in your devotion to God, bearing witness to the truth in all equity; and never let hatred of any-one lead you into the sin of deviating from justice. Be just: this is closest to being God-conscious. And remain conscious of God: verily, God is aware of all that you do.’ (Qur’an, Chapter 5, verse 8) After the talk had concluded,

people had left and only organisers and acquaintances mostly remained, I was approached by two students who informed me that they were writing an article on the 'Discover Islam Week.' I therefore obliged to answer their numerous questions, all of which however were to do with homosexuality and not the content of my talk. I clarified my position, which is that Islam holds sinful the act of homosexuality. It does not however mean that Muslims hate homosexuals. We are required to observe utmost decency and goodness with all. Although homosexuality is regarded as a sin and disliked in all religious discourse, Muslim, Jew and Christian, it does not warrant attacks or prejudice. I emphasised this point repeatedly so that the message was heard and understood. I felt that the two students who approached me came with a pre-set agenda and I made this clear to them during our discussion. It is sad and deplorable that such smear tactics were used even in an event whose topic sought to allay antagonisms. What followed was The Tab, the newspaper for which the two students were reporting, were intent on writing an article about me and another speaker. Members of the LGBT community were present at the talk and supported the Islamic Society and Student Union in releasing the following - http://www.impactnottingham.com/2014/03/lgbt-and-islamic-society-condemn-nottingham-tab-smear-tactics/

3) A lot of the ill-informed information about me and misquoting has come from the website Harry's Place. This was something I wrote in response to their accusations last year:

'Some points for the Islamaphobes at Harry's Place:

As for the quote asking for prayers for British-based poet Talha Ahsan, then this can never be considered a crime of any sort. The website http://freetalha.org/about/ was set up to petition for a fair trial for Talha in the UK. Those who have supported the initiative include his local MP and shadow justice secretary Sadiq Khan; novelist A L Kennedy and the civil rights organisation, Scotland Against Criminalising Communities (SACC). My support for him has always been based not on any alleged 'terror' offences', but on his right for a fair trial. This is the position of all who campaign for his release and trial in his home country of Britain.

As for Mohammed Hamid, then here is another dubious case, a case where Hamid and others were prosecuted and convicted of incitement to murder and running or attending terrorism training camps. As stated in a website set up to campaign for his release (http://freehamid.blogspot.co.uk/p/ipp.html), 'in reality, they went on camping trips, and went on a paintballing trip that was paid for as part of a BBC documentary…he was found guilty of "soliciting to murder" under legislation dating back to 1861, despite never actually instructing anyone to any specific act. The conviction was based upon innocuous statements allegedly made by Hamid whilst under covert surveillance which, by the accounts of those who appeared in court for the prosecution, were twisted to suit a government agenda." Encouraging prayers for Hamid and the signing of an online petition for his release can hardly be equated with supporting terrorism. Others who have rallied in support for him are the Irish Republican Prisoners Support Group (IRPSG), Fight Racism, Fight Imperialism, Cage Prisoners and Free Detainees.

As for the partial transcript from a talk on spying dating back to 2006 after the high publicity 2 June 2006 Forest Gate raid, not only is it 8 years old but it emerged in the context of a general fear in the London Muslim community that no other innocent family should be forced to go through the same treatment as the two brothers, particularly since one of the brothers had been shot by the police. The case was one that highlighted the failing of the Independent Police Complaints Commission for its failure to investigate how the police obtained the erroneous intelligence that led to the raid. At no point does Dr. Lateef excuse, glorify, promote or encourage any acts of terrorism or any violent behaviour against anybody. His words in that lecture undoubtedly however could have been better worded. He has attempted to have the lecture removed from Youtube by contacting the uploader but this has not yet proven successful.

As for Dr. Lateef speaking with Anwar al-Awlaki then we must really question the reasoning of Harry's Place, are people to be held guilty by association? Even Harry's Place stated that Dr. Lateef was a speaker with him before 'right up to 2009, when Awlaki had broadcast his allegiance to al-Qaeda for all to see'. So where is the controversy? Hundreds of speakers have shared platforms with Anwar al-Awlaki. In fact the last join program with Mr. Awlaki was on the theme of Companions of the Prophet Muhammad (peace be upon him), and this with video recordings of Mr Awlaki played at the event, and not with Awlaki in person. In fact Dr. Lateef has never physically met Mr. Awlaki.

To state unequivocally, Dr. Lateef has never excused, glorified, promoted or encouraged any act of terrorism at any of his hundreds of public lectures and weekly sermons. His campaigning is consistently one for justice for the oppressed, for Muslims and non-Muslims. It is to this end that he works alongside Interpal and with a host of many other charities including Cageprisoners.'

Please kindly take into consideration the aforementioned information. Please do not hesitate to contact me for any further information or clarification.

Yours Sincerely,

Uthman Lateef
March 2014

Supplementary written evidence submitted by Tom Keatinge [CT 33]

1 AUTHOR AND SUBMISSION INTRODUCTION

1.1 This submission is to supplement a paper previously submitted to the Committee[1] in light of my attendance at and viewing of the hearings held in connection with the recently closed 'Inquiry into Counter-terrorism.'

1.2 In particular, this contribution will focus on the nature of the current counter-terror finance ('CTF') regime, and will consider this effort in light of the extensive and timely focus the Committee applied to the question of 'foreign fighters' in particular in the context of the conflict in Syria.

1.3 The author recently left a near 20-year career in investment banking. His interest in and experience of counter-terror finance stems from a sabbatical year he spent in 2011/12 studying for a Masters at King's College London and continued, ongoing research and analysis he is conducting. His KCL Masters included a dissertation considering the effectiveness of the global 'Financial War on Terror' and the consequences of the counter-terrorist financing regime that has been implemented since 9/11. He was also the banking contributor to a report commissioned during the summer of 2013 by DfID in light of Barclays Bank's decision to terminate bank accounts for a number of UK-based Money Service Businesses (MSBs) and now researches and analyses matters concerning 'Finance & Security'.[2]

1.4 The author is writing in a personal capacity and in no way represents any organisation with which he has previously been or is currently involved. The expressed views are thus strictly his own.

[1] Available at http://www.parliament.uk/documents/commons-committees/home-affairs/CT%20Written%20Evidence.pdf

[2] More details are available at www.tomkeatinge.net

2 SURVEYING THE CURRENT CTF LANDSCAPE

2.1 Identifying terrorists' finances within a financial institution is extremely challenging. Flows are normally 'clean' and small (in contrast to the 'dirty' money laundered from the proceeds of crime).[3] In his 2012 testimony before the US House Committee on Homeland Security, Dennis M. Lormel who at the time of 9/11 was the Chief of the FBI's Counter-Terrorist Financing Operations Section noted that 'It is possible to identify terrorist financing, but highly improbable,'[4] and despite the immense amount of regulation developed in the context of CTF and the significant expense incurred by the financial services industry ('FSI') in terms of time, increased headcount, and systems upgrades, an extremely limited amount of terrorist financing has been revealed within the FSI.[5]

2.2 Within the UK, ownership of both the CTF policy and enforcement effort appears to be fragmented across a range of HMG Ministries and Agencies, with no obvious 'lead' ensuring that the various rules, regulations, policies, and strategies that are promulgated domestically and internationally are implemented and pursued in an effective manner.

2.3 The Independent Reviewer of Terrorism Legislation, David Anderson QC, highlights an example of this issue in his *Third Report on the Operation of The Terrorist Asset-Freezing etc Act 2010,* published in December 2013, noting that '[terrorist] asset-freezing is administered by a different department from other counter-terrorism powers.'[6] In light of his assessment, he raises the possibility (although refrains from recommending) that terrorist asset-freezing responsibilities should be transfered from HM Treasury to the Home Office where they would sit alongside the operation of other counter-terrorism measures.

2.4 This lack of coordination is also evident in the way in which the FSI is involved by the authorities in CTF efforts. The triennial *KPMG Global AML Survey*[7] in both 2011 and

[3] For example, according to FATF (2008), the 7/7 bombings are estimated to have cost a mere GBP8,000 http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Terrorist%20Financing%20Typologies%20Report.pdf

[4] Lormel, Dennis M (2012) Testimony to the US House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Lormel.pdf

[5] The total assets frozen by HM Treasury as of 30 September 2013 were a mere £82,000 under the Terrorist Asset-Freezing etc Act 2010 and £11,000 under EU Regulation (EC) 2580/2001. HM Treasury (2014), *Operation of the UK's Counter-Terrorist Asset Freezing Regime: 1 October 2013 to 31 December 2013* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/276397/WMS_1_October_2013_to_31_December_2013.pdf

[6] Anderson, David (2013), *Third Report on the Operation of The Terrorist Asset-Freezing etc Act 2010* para 2.24, p13

[7] KPMG (2011), *Global Anti-Money Laundering Survey: How Banks are Facing Up to the Challenge* https://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/global-aml-

2014 highlight the core issues: banks desire more guidance from and collaboration with the authorities in meeting their AML/CTF obligations. The one-way flow of information that currently exists is a counterintuitive and depressing state of affairs given that the authorities are relying on the FSI to be a front line of defence in counter-terrorism.

2.5 Richard Barrett, the former co-ordinator of the UN al-Qaeda and Taliban Monitoring Team, has underlined this point, stressing that 'States cannot expect the private sector to have a better idea of what terrorist financing looks like than the states themselves.'[8]

2.6 This lack of coordination and failure to leverage the capabilities of the FSI in support of the UK's counter-terrorism effort would seem, at best to be a missed opportunity and at worst a security weakness that needs to be challenged and addressed.

2.7 The FSI has highly advanced systems for screening money flows, account usage, and identifying unusual patterns. An everyday example is the way in which credit card issuers often block card usage which is inconsistent with a cardholder's normal habits, calling to confirm whether the owner of the card is aware of this unusual use.

2.8 Also instructive and of interest in this regard is the extent to which banks collaborate with the authorities in the fight against human-trafficking in the US, using the financial pictures they are able to develop with their data in conjunction with public agency guidance.[9]

3 FINANCING AND *JIHAD*

3.1 The vast majority of funds that are donated in support of groups operating in war zones such as Syria are given in response to the humanitarian tragedy created by these conflicts, and are donated via recognised and respected channels. However this is not always the case.

3.2 The global effort to starve al-Qaeda of financing has greatly diminished its ability to provide funding and resources to its affiliates, however its brand of ideology continues to appeal to donors around the world who seek opportunities to perform 'proxy *jihad*' via donating money in support of *jihadi* fighters.

---

survey-2011-main-report.pdf & KPMG (2014), *Global Anti-Money Laundering Survey* http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/global-anti-money-laundering-survey/Documents/global-anti-money-laundering-survey-v5.pdf

[8] Barrett, Richard (2012), 'Preventing the Financing of Terrorism' in *Case Western Reserve Journal of International Law* p730, Vol. 44, No. 3

[9] This short interview from May 2013 with Cyrus Vance, the Manhattan District Attorney, provides an insight into the collaborative efforts underway in the US. http://www.trust.org/item/20130502160826-lbpjr/

3.3 This concept of '*Tajheez al-Ghazi*' is a form of sponsorship which 'allows those who cannot, or will not, join the *Jihad* physically for whatever reason, to achieve the honour and heavenly reward of waging *Jihad* by proxy.'[10]

3.4 The December 2013 US Treasury designation order on Qatari-based Umayr al-Nu'aymi who is alleged to have channelled funding to a range of *jihadi* causes including ordering the transfer of nearly US$600,000 to al-Qaeda affiliates in Syria,[11] demonstrates that these deep-pocketed donors can, when attracted to a particular cause, gather and deliver significant funds, funds that are often transported into the battlefield by foreign fighters.[12]

3.5 It should thus be noted that foreign fighters also play an important cash-courier role as they travel to their chosen *jihadi* battlefield.

4 THE FSI IN THE CONTEXT OF *JIHAD* AND FOREIGN FIGHTERS

4.1 During the recently closed counter-terrorism enquiry, the committee has spent considerable time focused on the question of individuals that travel to *jihadi* theatres of operation, most notably Syria, and have questioned how a greater understanding can be built of who is travelling, when they leave/return, and what risk they might pose to the UK upon return.

4.2 Unpalatable as it may be to acknowledge at a time when data protection is a high profile topic, the FSI holds data that provides significant insight into the habits and movements of its account holders. Consider the way in which online retailers such as Amazon or loyalty card schemes such as Tesco Club Card can anticipate your purchasing interests – and this represents only a portion of an individual's financial transacting.

4.3 Clearly data protection and privacy issues are important when considering the use of any form of personal data and indeed the FSI has experienced fines and sanctions as a result of the loss or misuse of personal data. In the context of countering terrorist-financing, the proposed *4th EU Money Laundering Directive*[13] would appear to

[10] Dean, Aimen, Edwina Thompson & Tom Keatinge (2013), 'Draining the Ocean to Catch One Type of Fish: Evaluating the Effectiveness of the Global Counter-Terrorism Financing Regime', in *Perspectives on Terrorism*, Vol 7, No 4

[11] US Treasury (2013), *Treasury Designates Al-Qa'ida Supporters in Qatar and Yemen* http://www.treasury.gov/press-center/press-releases/Pages/jl2249.aspx

[12] It should be noted that travellers arriving in the UK from a country outside the EU, or leaving the UK to travel directly to a country outside the EU, must declare any cash of EUR10,000 or more (or its equivalent in other currencies). HMRC website: http://www.hmrc.gov.uk/customs/arriving/declaring-cash.htm

[13] European Union (2013), *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0045&from=EN

acknowledge the appropriate use of data held by the FSI in the context of addressing matters linked to AML/CTF stating in the accompanying *Explanatory Memorandum* that provisions are being introduced into the Directive 'to clarify the interaction between anti-money laundering/combating terrorist financing and data protection requirements.'[14]

4.4 The *Explanatory Memorandum* notes further: 'The processing of personal data should be permitted in order to comply with the obligations laid down in this Directive, including carrying out of customer due diligence, ongoing monitoring, investigation and reporting of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, sharing of information by competent authorities and sharing of information by financial institutions. The personal data collected should be limited to what is strictly necessary for the purpose of complying with the requirements of this Directive…'[15]

4.5 An appropriately constructed, intelligence-based public/private partnership with the FSI could thus enhance monitoring capabilities on a standalone basis, or be integrated with any work that may be undertaken using information (for example from 'geo-tagging') gathered from social media sources such as Twitter, Facebook, and YouTube to create a more accurate and refined picture of possible foreign fighter activity.

5 A Possible Parallel That Could Inform a Solution Model

5.1 In my previous submission, I drew attention to the 2013 announcement by HMG of plans to establish a Cyber Security Information Sharing Partnership (CISP) involving both public and private sector actors, and the possible utility of such a formalised forum in enabling collaboration between the FSI and the authorities.

5.2 Comments made by Francis Maude at the Chatham House launch seem to offer a structure that could also be applied to enhance the effectiveness of the CTF regime in the UK. In particular he highlighted[16] that 'CISP is all about: Government and industry working together to build a comprehensive picture of the cyber threat and coming up with the best defences' noting that 'The private sector...is the most important line of defence...' and that 'the Prime Minister [had] held an event...for senior executives, to underline the benefits of a real and meaningful partnership between industry and government.' He further noted that 'The government's proposal was this: by building a community of public and private partners, we could all pool our information on cyber threats and increase our visibility of cyber threats for mutual benefit.'

[14] Ibid. p7
[15] Ibid. p17
[16] Francis Maude (2013), https://www.gov.uk/government/speeches/cyber-security-information-sharing-programme

5.3 Most succinct and directly applicable to the current lack of partnership between regulatory/security authorities and the FSI was his conclusion: 'This kind of working is the future: government and industry working hand-in-hand to fight a common threat.'

6 THE FSI IS AN UNDERUTILISED SECURITY RESOURCE

6.1 *Recommendation*: the FSI is placed in a frontline 'financial border security' role by the authorities yet is an underutilised resource in the context of the UK's counter-terrorism strategy. HM Government would (1) benefit from establishing a partnership similar to the CISP that leveraged the significant capabilities of the FSI, and (2) with regards to the specific and immediate topic of foreign fighters, the FSI could also play a valuable role, guided by public sector agencies, in assisting with the identification of 'persons of interest' based on changes in their financial habits.

Tom Keatinge

March 2014

Supplementary written evidence submitted by the Home Office [CT 34]

Letter from James Brokenshire MP, Minister for Security and Immigration, to the Chair of the Committee, 28 March 2014

Following my appearance before your Committee on 18 March, you asked a number of follow up questions.

Overseas Capacity Building

FCO officials monitor and review the progress of individual capacity-building projects on a regular basis to assess whether they are on track to deliver their objectives and to ensure they are delivering value for money; and frequent progress reports are provided to Ministers. I welcome the fact that the Foreign Affairs Committee, in its 2012 report on the Government's human rights work, emphasised the significance of the accountability to Parliament and the wider public that flows from the Ministerial oversight of and approval for work of this nature.

The best measure of the effectiveness of these programmes is, of course, in the real-world improvements in capability they deliver for our partners overseas – and thus for our ability to protect the UK and its interests from terrorism in line with our human rights standards and obligations. We are already seeing our training help partners to disrupt terrorist planning overseas linked to the UK and to gather evidence that can be used effectively in court. We are also starting to see improvements in how terrorist cases are prosecuted overseas, with the development of specialist CT prosecutors and judges in several countries, effective handling of CT cases through the courts and improvements in CT investigators' evidence-gathering and forensics skills.

In respect of the scope of our projects, our main focus is on working with police, prosecutors, judges and prison authorities to build their capacity to investigate, detain, prosecute and convict terrorists based on respect for human rights and the rule of law. However, the FCO's CT Programme Fund covers a wide range of capacity-building work, including rule of law projects, aviation security and other areas that affect the UK or UK interests. For operational reasons we do not discuss the detail of projects that we fund.

The Global Counter-Terrorism Fun is a useful multilateral forum for progressing UK CT objectives. To date it has delivered benchmark standards in areas such as support for the victims of terrorism, effective criminal justice systems and denying the payment of ransom for kidnaps. It also designs and delivers capacity building programmes; but it does not act as a funding mechanism for those programmes. The UK is an active member of the GCTF, co-chairing its Countering Violent Extremism work-stream with the United Arab Emirates; and participating in its four other key work-streams: the Horn of Africa; the Sahel; crime, justice and the rule of law; and South-East Asia.

Bulk Data Collection

As you will appreciate, the policy of successive Governments is not to comment on sensitive national security issues and to neither to confirm nor deny the existence (or otherwise) of intelligence techniques or capabilities. The Government, however, has been very clear that the intelligence agencies must, and do, act in accordance with the law, a point that has been endorsed by the Intelligence and Security Committee (ISC) of Parliament. The ISC provides independent Parliamentary oversight to a range of national security issues. It is currently undertaking a far reaching review into Privacy and Security and I am sure that it will want to consider all aspects of relevant legislation.

You asked about Section 94 of the Telecommunications Act 1984. Directions under Section 94 can only be issued by a Secretary of State where he/she considers it is necessary to do so in the interests of national security. The legislation allows for such directions to be kept secret. It may be necessary to keep a direction secret because revealing its existence would damage national security. It is a matter for the ISC on how it exercises its oversight functions. I do not believe it would be appropriate to provide a commentary on how the Home Office has interacted with the ISC in relation to its requests.

In respect of your question on prior judicial authorisation, the Government believes that the UK has an effective system of safeguards in relation to interception and the work of the security and intelligence agencies more generally. We believe that the Government is best placed to make national security decisions, within a human rights-compliant legal framework, and that these decisions must be subject to independent and robust scrutiny and oversight, including from the judiciary. The current framework provides that. The ISC is reviewing the laws governing the work of the security and intelligence agencies, so I am sure that this is a further area that they will wish to consider.

<u>EU Nationals who have travelled to Syria</u>

I undertook to provide the sourcing for the figures I quoted in this session. The figure of 2,000 people thought to have travelled from the EU to Syria can be supported by a variety of open source reporting – many of which from counter terrorism experts. The International Centre for the Study of Radicalisation (ICSR) at Kings College estimated that as of December 2013 of 1,900 Western Europeans had travelled to Syria and, as I suggested in my evidence to the Committee, the EU Counter-Terrorism Coordinator Gilles De Kerchove has publically stated that more than 2,000 Europeans are likely to have travelled to Syria, noting that the largest numbers come from Belgium, Denmark, Germany, the Netherlands, and the UK. Since these were figures quoted at the beginning of this year, it is of course possible that the number may have increased since then.

James Brokenshire MP, Minister for Security and Immigration
March 2014

Written evidence submitted by Rt Hon Sir Malcolm Rifkind MP, Chairman, Intelligence and Security Committee [CT 35]

Letter from Rt Hon Sir Malcolm Rifkind MP, Chairman, Intelligence and Security Committee, to the Chair of the Committee, 6 February 2014

Thank you for your letter dated 28 January, inviting me to give evidence to your Committee on the work of the Intelligence and Security Committee of Parliament (ISC) and its role in overseeing the activities of the security and intelligence Agencies.

I have discussed the invitation with colleagues on the Committee and we have agreed that it would not be appropriate for me to accept. Parliamentary Committees are not usually called to give evidence on their work to another Committee. We would not seek to question you about your Committee's role overseeing the work of the Home Office - that, rightly, is your remit, just as oversight of the intelligence Agencies is ours.

Moreover, this Committee's oversight work has already, and very recently, been the subject of very detailed scrutiny by Parliament. The full House had a number of opportunities to debate the work of the ISC during the passage of the Justice and Security Act less than nine months ago. Parliament has therefore already discussed and agreed the Committee's role.

If it is information about our role which your Committee is seeking, then the relevant legislation is Part 1 and Schedule 1 of the Justice and Security Act 2013. However further information can be found in the ISC's last Annual Report. For your convenience I have enclosed both of these documents, which I trust you will find helpful.

In your letter you asked two specific questions about the Committee's staffing and access to the confidential annexes of the reports of the Intelligence Services Commissioner and the Interception of Communications Commissioner, both of which I am happy to answer.

The ISC currently has eight full-time members of staff and a part-time Investigator. We currently have four full-time vacancies and three part-time vacancies which we are in the process of filling. Our total complement will therefore be twelve full-time and four part-time members of staff. In addition, Government will be providing the Committee with a separate team of five individuals to carry out the separate work arising from the Gibson Inquiry,

I can confirm that the Committee has access to all the material in the Commissioners' annexes that falls with its remit (so, for example, we would not wish to receive any material which related to bodies which do not fall within our remit).

Rt Hon Sir Malcolm Rifkind MP, Chairman,
Intelligence and Security Committee
February 2014