Counter-Terrorism Policy Initiatives:

Main Areas of Concern

Contents

1. Introduction
2. Terrorist Finance Tracking Programme
3. Passenger Name Record
4. Terrorist Lists
5. Extraordinary Rendition, Secret Detention and Complicity in the Use of Torture
6. The Internet and Counter-Terrorism
7. Conclusions and Recommendations

1. Introduction

This briefing paper, 14b, complements briefing paper 14a, which looked at the legal and policy framework developments since 2005, in the area of EU counter-terrorism. 14b will focus on some of the specific policies that have been implemented, or developed, over the last five years. It will examine the most serious concerns – relating to human rights, civil liberties, and peace issues - which surround them, ending in a set of recommendations.

2. Terrorist Finance Tracking Programme

The Terrorist Finance Tracking Programme (TFTP) or "SWIFT" agreement is an anti-terrorism measure which allows US authorities to request and, upon the approval of Europol (who can thereafter also gain access), large volumes of transaction information from SWIFT. SWIFT – the Belgian Society for Worldwide Interbank Financial Telecommunication – is the inter-service banking company used in roughly 80 per cent of international transactions.[1] The agreement was signed on 28 June 2010 and entered into force on 1 August 2010, and is intended to support the prevention, investigation, detection, or prosecution of terrorism or terrorist financing.[2] Since its conception it has been subject to concerns about transparency, fundamental rights (including to the protection of personal data) and the principles of proportionality and necessity.

Prior to its signature in June 2010, an interim agreement on SWIFT transfers had been rejected by the European Parliament, using its new powers under the Lisbon Treaty. MEPs had demanded various changes to the original text, concerning the bulk transfer of data, the creation of an EU counterpart to the US's TFTP, and EU oversight of TFTP data requests.[3]

---

[1] Summarised from Vogel, Toby, 'EU, US sign SWIFT agreement' in *European Voice*, 28 June 2010, [online] accessed July 2011, available at http://www.europeanvoice.com/article/2010/06/eu-us-sign-swift-agreement/68367.aspx

[2] For more information, see the Official Journal of the European Union, *Agreement Between the European Union and The United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for Purposes of the Terrorist Finance Tracking Program,* L 195/1, Volume 53, 27 July 2010, [online] accessed October 2011, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0001:0002:EN:PDF

[3] Summarised from Digital Civil Rights in Europe, *SWIFT agreement implementation not respecting data protection safeguards,* 9 March, 2011, [online] accessed July 2011, available at http://www.edri.org/edrigram/number9.5/swift-agreement-data-protection-safeguards

These changes were, in various forms, eventually accepted by the Council of the EU and by the US. However, the controversy did not end there.

Transparency was one of the key issues in the controversial agreement, and the final agreement allows the transfer of data pertaining to European bank customers to US investigators *only in accordance with strict guidelines*. The task of EU oversight of TFTP data requests was given to Europol, the EU Agency for the prevention and combat of organised crime, terrorism and other forms of serious crime, affecting two or more Member States (despite the fact that the negotiating mandate stipulated that it should be given to a judicial public authority). Not only is Europol not a judicial public authority, it also has specific interests in the exchange of personal data, on the basis of the agreement. Article 10 of the agreement gives Europol the power to make requests for relevant information obtained through the TFTP, if it has a reason to believe that a person or an entity has a nexus to terrorism. It has been noted by the European Data Protection Supervisor (EDPS) that:

> *"It is hard to reconcile this power of Europol, which may be important for the fulfilment of Europol's task and which requires good relations with the US Treasury, with the task of Europol to ensure independent oversight."*[4]

Europol must ascertain if a US request meets the criteria in the agreement before agreeing to supply the data. However, it has transpired in the first year of the agreement's functioning that many provisions of those guidelines have been widely ignored. A critical report from the Europol Joint Supervisory Body (JSB) noted that the written requests received by Europol from the US are too vague to decide on their validity.[5] Yet despite the shortcomings, Europol has agreed to every request. In effect:

> *"Europol seems to be just "rubberstamping" requests for the transfer of raw data without any scrutiny or oversight. Authorisation of these bulk transfers seems to be on the basis of oral, unrecorded requests, and all documents have so far been classified as top secret."*[6]

The JSB report complained that this makes oversight of data privacy and of adequate internal and external audit of the necessity and proportionality of data transferred to the US, "impossible".[7] Article 4 of TFTP requires requests to be limited in scope and to come with adequate written explanation,[8] but the requests have been granted despite, according to the JSB report, not being specific enough to allow Europol to decide whether to approve

[4] European Data Protection Supervisor (EDPS), *Opinion on the Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II),* 22 June 2010, p. 6

[5] Europol Joint Supervisory Body (JSB), *Report on the Inspection of Europol's Implementation of the TFTP Agreement*, conducted in November 2010, Report No. JSB/Ins. 11-07, Brussels, 1 March 2011

[6] Digital Civil Rights in Europe*, ibid.*

[7] JSB Report, *ibid.*

[8] Article 4 - U.S. Requests to Obtain Data from Designated Providers. Section 2. 'The Request (together with any supplemental documents) shall:
(a) identify as clearly as possible the data, including the specific categories of data requested, that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing;
(b) clearly substantiate the necessity of the data;
(c) be tailored as narrowly as possible in order to minimize the amount of data requested, taking due account of past and current terrorism risk analyses focused on message types and geography as well as perceived terrorism threats and vulnerabilities, geographic, threat, and vulnerability analyses; and
(d) not seek any data relating to the Single Euro Payments Area.' (TFTP Agreement*, ibid.*)

or deny them. US requests have been too general and too abstract to allow proper evaluation of the proportionality and necessity of the requested data transfers, and at times based on orally-provided information to certain Europol officials with the stipulation that no record is made. This prevents the JSB from checking whether Europol could have rightly come to its decisions and therefore makes external audit by both the EDPS and JSB, as required by the TFTP Agreement, impossible.[9] The JSB therefore recommends that all requests be provided in written form and the US Department of the Treasury be contacted to ensure requests are sufficiently detailed, including supplemental documents where necessary.[10]

Article 13 of the TFTP also requires that a joint review is carried out by the Commission and the US authorities to assess the status of implementation. This review, although less critical than the JSB report, published in March 2011, also 'recommends that as much (classified) information as possible substantiating the requests is provided to Europol in a written format in order to support it in its tasks under Article 4 and to allow for more effective independent review.'[11] It also recommends the provision of more publicly accessible information on the way the programme functions (in particular the overall volume of data provided to the US authorities, and the number of financial payment messages accessed), in as far as this is possible without endangering its effectiveness. More verifiable statistical information on the added value of TFTP derived information to efforts to combat terrorism and its financing are required in order to 'further substantiate the added value of the program'.[12]

A further concern is that a second control mechanism stipulated in the agreement appears to have failed. Article 15 states that every EU citizen has the right to know if US authorities have had access to their personal banking data and if so, which authorities received that information. However, an effort by a German MEP Alexander Alvaro, the Parliamentary rapporteur on the TFTP agreement, to determine if US officials had accessed his personal account information failed. For six months the German authorities failed to find out whether data had been accessed at all. 'As such, the rights of EU citizens on correction, deletion or blockage of the data are being violated.'[13] It has been suggested that without the possibility of individual redress or access to information on which data has been processed, this agreement is not in line with Europe's constitutional principles or laws, and could be taken to the European Court of Justice, European Court of Human Rights or Member State level courts.

Overall, the European Parliament has been extremely dissatisfied with the TFTP's implementation, claiming that it makes their hard-won concessions meaningless, and threatening to withdraw their support. The Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) held a public hearing on these matters in March 2011.[14] The

---

[9] Statement summarised from Europol Joint Supervisory Body (JSB), *US and EU agreement on exchanging personal data for the purposes of the Terrorist Finance Tracking Program (the TFTP Agreement) – first inspection performed by the Europol Joint Supervisory Body (JSB) raises serious concerns about compliance with data protection principles.* Website Notice, Brussels, 2 March 2011, [online] accessed October 2011, available at http://europoljsb.consilium.europa.eu/media/112160/jsb%20tftp%20inspection%20-%20website%20notice,%20march%202011.pdf

[10] Recommendation summarised from JSB Report, *ibid.*

[11] Europol Public Information, *Europol Activities in Relation to the TFTP Agreement Information Note to the European Parliament 1 August 2010 – 1 April 2011*, The Hague, 8 April 2011, File no. 2566-566, quoting the European Commission review report published on 17 March 2011, [online] accessed October 2011, available at http://www.statewatch.org/news/2011/apr/eu-europol-report-on-implementation-tftp-agreement.pdf

[12] JSB Website Notice, *ibid.*

[13] Schult, Christoph 'Problems with Transparency: Brussels Eyes a Halt to SWIFT Data Agreement' in *Der Speigal*, 16 March 2011, [online] accessed July 2011, available at http://www.spiegel.de/international/europe/0,1518,751262,00.html

[14] See European Parliament Press Release, *SWIFT implementation report: MEPs raise serious data protection concerns*, LIBE Committee Meeting, 16 March 2011, [online] accessed October 2011, available at http://www.europarl.europa.eu/en/pressroom/content/20110314IPR15463/html/SWIFT-implementation-report-MEPs-raise-serious-data-protection-concerns

Committee expressed their dismay that the agreed EU oversight of TFTP data-processing was given to Europol, with one MEP suggesting that entrusting this task to Europol "is like putting the fox in charge of the chicken coop".[15] It is inappropriate for Europol to be the body who make the decisions on whether US request meet TFTP criteria, as they are the ones who will benefit from whatever the data unearthed might lead to. The LIBE Committee also called for a Commission proposal for data extraction on European soil rather than bulk transfer to the US.

The European Data Protection Supervisor (EDPS) has made this recommendation as well:

> *"solutions should be found to ensure that bulk transfers are replaced with mechanisms allowing financial transaction data to be filtered in the EU, and ensuring that only relevant and necessary data are sent to US Authorities. If these solutions could not be found immediately, then the Agreement should in any event strictly define a short transitional period after which bulk transfers are no longer allowed."*[16]

The EDPS has further questioned to what extent the agreement is necessary in order to obtain results that could be obtained by using less privacy-intrusive instruments. To meet European Data Protection laws, the processing of personal data must be necessary and proportionate. There are several existing instruments in the EU and international framework, containing a number of measures aimed at combating the misuse of the financial system for the purpose of money laundering and terrorist financing.[17] These instruments also contain specific provisions allowing exchange of information with third countries authorities as well as safeguards for the protection of personal data, in line with Directive 95/46/EC.

The EDPS notes that the Commission has highlighted the *usefulness* of the TFTP, but that the condition laid down by Article 8 ECHR in order to justify interference with private life is "necessity" rather than "usefulness". Therefore, further evidence is required of the real added value of this agreement, taking into account already existing instruments. Even if necessity is demonstrated, the bulk data issue still needs to be properly addressed, and there is another proportionality concern surrounding the storage period. TFTP enables the US authorities to store the data for a period of five years irrespective of whether they have extracted information from it or there is a proved link with a specific investigation or prosecution.[18]

The EDPS also notes that 'to enhance the effectiveness of both the oversight (Europol) and the joint review (Commission and US authorities), information and relevant data should be available on the number of access and redress requests, possible follow-up (deletion, rectification, etc.), as well as the number of decisions limiting rights of data subjects. In the same way, as far as the review is concerned, information should be available and reported

[15] *ibid.*
[16] EDPS 2010, *ibid.* p. 5
[17] In particular, Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Regulation (EC) 1781/2006 on information on the payer accompanying transfers of funds. Furthermore, the agreement on mutual legal assistance between the EU and the US explicitly allows the exchange between law enforcement authorities of information relating to bank accounts and financial transactions, and it provides conditions and limitations with regard to this exchange. Also at international level, the so-called Egmont Principles (see http://www.egmontgroup.org/library/download/5) set the basis for the international exchange of financial transactions information between Financial Intelligence Units, while establishing limitations and safeguards with regard to the use of exchanged data. In addition, instruments for the exchange of data between the US and Europol and Eurojust are already in place, ensuring at the same time exchange of information and protection of personal data. Summarised from EDPS, 2010 *ibid.,* pp. 3-4
[18] Summarised from *ibid.,* p. 4

on the quantity not only of messages "accessed" by the US Treasury but also of the messages "provided" to the US Treasury.'[19]

QCEA echoes the concerns and recommendations of both the LIBE committee and the EDPS regarding necessity and proportionality, independent oversight and the end to bulk transfer of data.

3. Passenger Name Record

The Passenger Name Record (PNR) has also been a controversial issue since its conception. PNR data is information provided by airline passengers, and collected by the air carriers for their own commercial purposes. It contains several different types of information, such as travel dates, travel itinerary, ticket information, contact details, travel agent at which the flight was booked, means of payment used, seat number and baggage information.[20] It can also include information about meal preferences, including where such preferences are for religious reasons, medical conditions and other sensitive personal data. PNR data has been used in customs and law enforcement for many years, but it is only recent technological developments that have opened up the possibility of being used in a more systematic manner.

Since 2001, the US government has increasingly used both real-time and archived PNR data to investigate and prevent terrorist attacks, and has sought to collect, transfer and retain PNR data from carriers flying into the US. The transfer to the US authorities of PNR data held by European airlines has been the subject of successive agreements since the early 2000s. There are currently provisional PNR agreements with the US, Canada and Australia. These have not yet been officially concluded by the EU, as upon the entry into force of the Treaty of Lisbon, the European Parliament proposed that the US and Australia Agreements should be renegotiated as they do not provide for adequate protection of personal data, and the Canada agreement is also due to be renegotiated as it expired in 2009.[21]

The history of PNR provides a useful context for the concerns with it today. One of the first EU-US PNR Agreements, signed in May 2004, was later annulled by the European Court of Justice, following a case brought by the European Parliament, who had strong objections to the Agreement on data protection grounds.[22] In November 2007, a new and contentious PNR proposal was adopted by the Commission for a Council Framework Decision on the use of PNR data for law enforcement purposes.[23] The consultation on this Framework Decision revealed significant reservations and objections from several actors, including the European Parliament and the EDPS:

The European Parliament Resolution of the 20 November 2008 stated that the need for the proposed actions had not been sufficiently demonstrated, and questioned whether the proposal met the standard required for justifying an interference with the right to data protection. The Resolution expressed Parliament's concern that the added value of the proposal in the light of other border initiatives had not been assessed. Regarding data

[19] *ibid.*, p. 8
[20] Summarised from Europa Press Releases, *EU Passenger Name Record (PNR) - Frequently Asked Questions*, [online] accessed October 2011, available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/60
[21] Summarised from European Commission, *Impact Assessment Accompanying Document To The Proposal For A European Parliament And Council Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Commission Staff Working Paper, Brussels, SEC(2011) 132, [online] accessed October 2011, available at http://www.statewatch.org/news/2011/feb/eu-com-eu-pnr-ia-sec-132-11.pdf
[22] For more information, see European Court of Justice, *Judgment Of The Court Of Justice In Joined Cases C-317/04 And C-318/04,* Press Release No. 46/06, 30 May 2006, [online] accessed October 2011, available at http://www.statewatch.org/news/2006/may/coj-judment-eu-us-pnr.pdf
[23] European Commission, PNR Impact Assessment, 2011*, ibid.*

protection, Parliament called for a clear purpose limitation and emphasised that only specific authorities should have access to PNR data. Finally Parliament expressed concerns that the proposed method of automatically assessing PNR data using fact-based pre-determined assessment criteria was a very wide use of the data and stressed that such assessment should never result in 'profiling' on the basis of sensitive data.

The Article 29 Data Protection Working Party[24] considered that the proposal was disproportionate and that it might violate the right to data protection. It called into question the data protection regime as Framework Decision 2008/977/JHA does not cover domestic processing of data. It considered that the demonstration of the need for the proposal was inadequate, that the data retention period (13 years) was disproportionate and that only the 'push' method of data transfer should be used (i.e. data is not automatically transferred, but specific data given on request).

The European Data Protection Supervisor questioned whether the necessity and proportionality of the proposal had been demonstrated since the proposal concerns the collection of data of innocent persons. He criticised the proposal as contributing towards a surveillance society and also called into question the data protection regime as domestic processing of data is not covered by Framework Decision 2008/977/JHA. The EDPS specifically suggested better defining the authorities that would have access to PNR data and the conditions for transferring data to third countries.

The Fundamental Rights Agency was also of the opinion that the necessity and proportionality of the proposal had not been demonstrated and considered that there should be more guarantees in the proposal in order to avoid profiling on the basis of sensitive data.[25]

Because of these issues and the controversy surrounding the 2007 proposal, the Commission proposal was not adopted by the Council before the entrance into force of the Lisbon Treaty in December 2009. The 2007 proposal was then obsolete because of the change to the legal basis and the decision-making procedure, from consultation to the co-decision procedure.[26] However, the Stockholm Programme mandated a PNR proposal from the Commission, and in February 2011 the Commission duly published one, with the stated aim to 'harmonise Member States' provisions on obligations for air carriers, operating flights between a third country and the territory of at least one Member State, to transmit PNR data to the competent authorities for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.'[27]

It has been recognized that the 2011 proposal is an improvement on the 2007 proposal, and has taken into account some of the feedback, including:

- stricter limitation of the purpose of using the data;
- a stronger data protection regime with a specific retention period and prohibition of the use of sensitive data, such as data revealing a person's race or ethnic origin,

[24] Article 29 of the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) created the "Working party on the Protection of Individuals with regard to the Processing of Personal Data," commonly known as the "Article 29 Working Party". The Working Party gives advice about the level of protection in the European Union and third countries, and is made up of a representative from the data protection authority of each EU Member State, the EDPS and the European Commission.
[25] This list is a summary of information contained in European Commission, *Proposal for a Directive Of The European Parliament And Of The Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.* Brussels, 2 February 2011, COM(2011)132 final, p. 10
[26] Information from PNR Impact Assessment 2011, *ibid.*
[27] PNR Commission Proposal 2011, *ibid.*

religious or philosophical belief, political opinion, trade union membership, health or sexual life;
- the 'push' method, with strict limitations on onward transfers of data to third countries;
- clear limitation of the scope of the proposal to air transport.

The new proposal also notes that whilst some stakeholders were not convinced of the necessity of using PNR data, they all agreed that legislation at EU level is preferable to the development of diverging national PNR systems.[28] It is argued that an EU-wide PNR agreement will harmonise national systems in order to avoid up to 27 considerably diverging systems being created, as several Member States have, following on from the UK's example, been preparing their own PNR legislation. This, it is stated, could result in uneven levels of protection of personal data across the EU, security gaps, increased costs, and legal uncertainty for passengers and carriers.[29]

For the breach of data protection to be legal, it must be demonstrated to be necessary. The 2011 proposal states that:

> ***"in the absence of harmonised provisions on the collection and processing of PNR data at EU level, detailed statistics on the extent to which such data help prevent, detect, investigate and prosecute serious crime and terrorism are not available.***
>
> *The necessity of using PNR data is however supported by information from third countries as well as Member States that already use such PNR data for law enforcement purposes. The experience of those countries shows that the use of PNR data has led to critical progress in the fight against in particular drugs, human trafficking and terrorism, and a better understanding of the composition and operations of terrorist and other criminal networks.*
>
> *With respect to drugs, Member States have indicated that the majority of seizures are made due to the use of PNR data in real-time and pro-actively. Belgium reported that 95% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data. Sweden reported that 65-75% of all drugs seizures in 2009 were exclusively or predominantly due to the processing of PNR data."*[30]

The proposal also states that whilst there are various existing provisions in the same area, including Advance Passenger Information (API), Schengen Information System (SIS – I & II), and Visa Information System (VIS), the purposes and uses of PNR are different and not covered by these existing mechanisms. API is used mainly to fight irregular immigration and facilitate border controls, SIS I & II for apprehending wanted persons, and VIS for verifying identities of known suspects (although they can, variously and under certain conditions, be used for law enforcement purposes).[31] PNR uniquely will enable law enforcement authorities to conduct an advance assessment of passengers, and therefore facilitate the detection of hitherto 'unknown' criminals or terrorists, based on predetermined assessment criteria.

However, the EDPS remains dissatisfied with the 2011 proposal. He has stated that:

[28] Above list summarised from PNR Commission Proposal 2011, *ibid.* pp. 10-11
[29] This was noted in the PNR FAQ, *ibid.*
[30] PNR Commission Proposal 2011, *ibid.* p. 6
[31] For more information on these existing instruments, see PNR Commission Proposal 2011, *ibid.* pp. 6-8

"the essential prerequisite to any development of a PNR scheme - i.e. compliance with necessity and proportionality principles - is not met in the Proposal… PNR data could certainly be necessary for law enforcement purposes in specific cases and meet data protection requirements. It is their use in a systematic and indiscriminate way, with regard to all passengers, which raises specific concerns.

"The Impact Assessment gives elements aiming at justifying the need for PNR data to fight against crime, but the nature of this information is too general, and it fails to support the large scale processing of PNR data for intelligence purposes. In the view of the EDPS, the only measure compliant with data protection requirements would be the use of PNR-data on a case-by-case basis, when there is a serious threat established by concrete indicators."[32]

Furthermore, the EDPS expresses more specific concerns, including that:

- The scope of application should be much more limited with regard to the type of crimes involved. The EDPS questions the inclusion in the Proposal of serious crimes which have no link with terrorism. In any case, minor crimes should be explicitly defined and ruled out. The EDPS recommends excluding the possibility for Member States to widen the scope of application;
- No data should be kept beyond 30 days in an identifiable form, except in cases warranting further investigation;
- The list of PNR data to be processed should be reduced; in particular, the "general remarks" field (meal preferences, health conditions etc) should not be included;
- The evaluation of the Directive should be based on comprehensive data, including the number of persons effectively convicted - not merely prosecuted - on the basis of the processing of their data.
- The developments on EU PNR should be assessed in a broader perspective including the ongoing general evaluation of all EU instruments in the field of information exchange management launched by the Commission in January 2010. In particular, the results of the current work on the European Information Exchange Model expected for 2012 should be taken into consideration in the assessment of the need for an EU PNR scheme.[33]

Whilst the EDPS's concerns are clearly serious and should undoubtedly be taken seriously, there is another issue that is of concern regarding fundamental rights; the right to non-discrimination.

The explicit uses by law enforcement authorities of PNR data are:

- **reactive:** use in investigations, prosecutions, unravelling of networks after a crime has been committed. In order to allow law enforcement authorities to go back sufficiently in time, a commensurate period of retention of the data by law enforcement authorities is necessary;
- **real-time:** use prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed. In such cases PNR data are necessary for running against predetermined assessment criteria in order to identify previously

[32] European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, Brussels, 25 March 2011

[33] This is a summary of some of the EDPS's recommendations - for the full recommendations, see *ibid.*

'unknown' suspects and for running against various databases of persons and objects sought;

- **proactive:** use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers. In order to carry out such an analysis of relevance for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, a commensurate period of retention of the data by law enforcement authorities is necessary.[34]

There is a concern here that the same data is to be used in the creation and use of so-called "objective" assessment criteria to identify 'unknown' suspects – in other words, profiling people on the basis of fitting certain criteria or matching certain patterns. The Impact Assessment noted that:

> *"one of the biggest criticisms of the use of PNR data for trend analysis and for running it against the fact-based assessment criteria is that it might result in what is critically referred to as 'profiling'. Profiling can be described as an automatic data processing technique that consists of applying a "profile" to an individual, in order to take decisions affecting him or her."*[35]

The Impact Assessment also notes that EU data protection legislation protects any individual from being subject to a decision which produces legal effects, based exclusively or to a decisive extent on automated processing of data. The 2011 proposal therefore includes a provision that any automated individual decision has to be reviewed by non-automated means before action is taken.[36]

The 2011 proposal also addresses, in a roundabout way, what it supposes to be the concerns of profiling based on nationality or skin colour, and states that:

> *"the use of PNR data prior to arrival allows law enforcement authorities to conduct an assessment and perform a closer screening only of those persons who are most likely, based on objective assessment criteria and previous experience, to pose a threat to security. This facilitates the travel of all other passengers and reduces the risk of passengers being subjected to examination upon entry into the EU on the basis of unlawful criteria such as nationality or skin colour which may wrongly be associated with security risks by law enforcement authorities, including customs and border guards."*[37]

However, there is still a lack of transparency or explicitness about what these objective assessment criteria might be. Moreover, regardless of the basis on which profiling takes place, be it nationality, skin colour or flight patterns, the major issue is the number of innocent people who will fit such patterns or criteria (whatever they are, or are based upon) and may therefore be subject to interrogation or other action on this basis. Merely having a person review an automated procedure does not alter this fact. Therefore, despite some progress in this area, it cannot yet be said that concerns over profiling have been resolved. Law must be explicit, not vague, yet this notion of automated processing and analyzing PNR data is based on unspecified terrorist expertise, experience or intelligence. There is also an

[34] Summarised from PNR Commission Proposal 2011, *ibid.* pp. 3-4
[35] PNR Impact Assessment 2011, *ibid.* p. 25
[36] See PNR Commission Proposal 2011, *ibid.* p. 22
[37] PNR Commission Proposal 2011, *ibid.* p. 5

apparent circularity in suggesting that the very same PNR data that has these 'objective assessment criteria' applied to it will also be used to create it.

There has recently been a further scandal surrounding PNR. As noted above, there are currently PNR agreements between the EU and three third countries, the United States, Canada and Australia, which are provisionally applicable. In September 2010, the European Commission adopted a package of proposals on the exchange of PNR data with third countries, consisting of an EU external PNR strategy and recommendations for negotiating directives for new PNR agreements with these three countries.[38] Negotiations have since started and are ongoing.[39] In June 2011 however, following the leak of a Council document containing a draft EU-US agreement,[40] it was reported that the Commission's legal team have warned that the draft agreement would be illegal.[41] The note by the Commission's legal service, dated 16 May, says it has "grave doubts" that the passenger name record (PNR) deal, now being finalised, complies with the fundamental right to data protection. The most serious concerns include:

- **The widely-drawn limits on the use of the personal data**. The US-European PNR database is being built "to prevent and detect terrorism and serious crime" but the lawyers say this definition includes any offence carrying a jail term of more than 12 months: "Given the low maximum penalty, it is likely to include a very large number of crimes which cannot be regarded as serious. This point alone puts the proportionality of the agreement in question." The PNR database can also be used "to ensure border security", by identifying people who should be subject to closer questioning on entering or leaving the US. The lawyers say this means the database can be used to investigate minor immigration or customs offences without any link to terrorism or serious crime; [42]
- **The disproportionate storage period of 15 years.** The 15-year retention period – four times longer than the current deal – includes five years on an "active" database, after which information will be archived in a "dormant" database for 10 years, though still accessible to senior law enforcement agents. The lawyers say 15 years goes "far beyond" the five years in the EU's own proposal for internal European travel, and the five and a half years in a proposed deal with Australia: "The council legal service in its opinion on EU-PNR ... questioned the necessity of a period of more than two years. It appears highly doubtful that a period of 15 years can be regarded as proportional."[43] Comparatively, the German constitutional court ruled in 2010 that six months was the maximum appropriate period for retaining personal telecommunications data;[44]
- **The lack of independent oversight and proper access to the courts for those seeking judicial redress over misuse of their details**. '"All redress is made subject to US law, while the forms of redress explicitly guaranteed are administrative only and thus at the discretion of the department of homeland security." Oversight to be

[38] For more information see, Europa Press Releases, *European Commission adopts an EU external strategy on Passenger Name Record (PNR),* Brussels, 21 September 2010, IP/10/1150, [online] accessed October 2011, available at http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1150&format=HTML&aged=1&language=EN&guiLanguage=fr

[39] This is noted in the PNR FAQ, *ibid.*

[40] The leaked document is: Council of the European Union, *Note from the Presidency to the delegations, on a Draft Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record data to the United States Department of Homeland Security*, Brussels, 20 May 2011, 10453/11, Restreint UE, [online] accessed August 2011, available at http://www.guardian.co.uk/world/interactive/2011/may/26/privacy-us-national-security

[41] As noted by Travis, Alan, 'Air passenger data plans in US-EU agreement are illegal, say lawyers' in *the Guardian*, 20 June 2011, [online] accessed August 2011, available at http://www.guardian.co.uk/world/2011/jun/20/air-passenger-data-plans-illegal?INTCMP=SRCH

[42] Summarised from *ibid.*

[43] *ibid.*

[44] Information from *ibid.*

carried out by homeland security "privacy officers" does not amount to independent oversight, say the European [Commission] lawyers'.[45]

Statewatch, an organization which monitors civil liberties across Europe, has noted that:

> *"Secret minutes of EU-US meetings since 2001 show that they have always been a one-way channel, with the US setting the agenda by making demands on the EU. When the EU does make rare requests, like on data protection, because US law only offers protection and redress to US citizens, they are bluntly told that the US is not going to change its data protection system – as they were at the EU-US JHA ministerial meeting in Washington on 8-9 December 2010."*[46]

Statewatch has recommended that the European Parliament should refuse its consent to the agreement in its current form. Given that the legal advice concludes that despite 'certain presentational improvements, the draft agreement does not constitute a sufficiently substantial improvement of the agreement currently applied on a provisional basis, the conclusion of which was refused on data protection grounds by the European Parliament',[47] it seems consistent and appropriate that the Parliament should deny its approval until these issues are substantively addressed.

Another issue that has caught press attention recently is the possibility that PNR be extended to flights within the EU – intra-European flights. These are currently not included, but the 2011 proposal mandates a special review of the potential extension to internal EU flights.[48] Some Member States - notably the UK, who have been leading the campaign – believe PNR should be extended internally, so as to preclude security gaps, given that in some Member States 70% flights are intra-EU, and terrorists may use EU hubs instead of direct international flights, as the complexity of their journeys increases. However, other Member States such as Germany have expressed concerns that this would contravene EU laws on the free movement of persons enshrined in the *acquis communautaire*.[49]

QCEA shares the concerns of the Parliament, the EDPS, the Data Protection Working Party, and civil liberties organizations like Statewatch, and urges the Commission and Council to reflect on the recommendations made by them regarding PNR. QCEA urges the Parliament to continue exercising its scrutiny and to uphold its commitment to the realization of the fundamental rights enshrined in the Treaties of the EU.

4. Terrorist Lists

Terrorist listing or proscription is 'the act of designating a group or individual as terrorist, as an associate of known terrorists, or as a financial supporter of terrorism' which is 'designed to disrupt the activities of terrorist groups by criminalising their members, cutting off their access to funds and undermining their support'.[50] Terrorist lists originate at UN, EU and Member State level, but regardless of the source 'the effects on the lives of blacklisted

[45] *ibid.*
[46] Bunyan, Tony, Statewatch, in Travis 2011, *ibid.*
[47] Travis 2011, *ibid.*
[48] PNR Comission Proposal 2011, *ibid.* p. 13
[49] Summarised from EurActiv, *EU rallies behind UK on collecting air passenger data*, 31 March 2011, [online] accessed August 2011, available at http://www.euractiv.com/en/justice/eu-rallies-uk-collecting-air-passenger-data-news-503646
[50] Sullivan, Gavin and Hayes, Ben, *Blacklisted: Targeted sanctions, preemptive security and fundamental rights,* European Center for Constitutional and Human Rights (ECCHR), 2010, p. 6, [online] accessed October 2011, available at http://www.ecchr.eu/publications/articles/blacklisted-targeted-sanctions-preemptive-security-and-fundamental-rights.864.html

individuals are largely the same - namely, all their financial assets are frozen, their travel and freedom of movement are severely restricted and their everyday lives (as well as those of their families) are devastated'.[51] Although it is 'widely accepted that the lists have been largely ineffective in blocking terrorist financing, states have nonetheless prioritised blacklisting as a means of facilitating prolonged interference with the lives of terrorist suspects on the basis of intelligence material incapable of withstanding judicial scrutiny.'[52]

"The UN blacklisting regime stems from UN Security Council Resolution 1267, which created the first list of alleged terrorists "associated with Osama bin Laden, the Taliban and Al-Qaeda". Those included in the list (which currently stands at 397 individuals and 92 organisations) are subject to asset-freezing, travel bans, an arms embargo and other sanctions. UN Security Council Resolution 1373, adopted in the immediate aftermath of 11 September 2001, encouraged states to create their own blacklists to prevent "the financing of terrorist acts" and enact other counter-terrorism provisions criminalisingsupport for terrorism and breaches of the UN sanctions. The EU's terrorist lists stem from the measures it took to transpose Resolution 1373 into EU law and currently stands at 57 individuals and 47 organisations. In addition to the UN and EU lists, many states have adopted domestic blacklists, massively expanding the net of criminalisation."[53]

The UN lists are not based on any agreed definition of terrorism, which 'effectively outsources the definition of terrorism to nation states, encouraging the criminalisation of groups on the basis of geopolitical, foreign policy or diplomatic interests.'[54] The EU list is based on a very broad definition of terrorism, which is therefore also open to politically or ideologically motivated listings. Lack of, or broadness of, definition, without clarity over what link a state must demonstrate between an individual/group and the 'terrorist acts' they are reputedly connected to, has led to 'guilt by association,' 'categorical suspicion' (regardless of whether it can be shown to be founded) and lack of access to judicial review (i.e. precluding the possibility of suspects being able to demonstrate their innocence) becoming the operative principles of blacklisting regimes.[55]

There is a large and growing body of expert legal opinion and judicial rulings which views these proscription regimes as incompatible with basic standards of due process. Decisions to add an individual or organization to a list are usually based on secret intelligence material that neither blacklisted individuals nor the courts responsible for reviewing them will ever see. Clearly, affected parties cannot contest the allegations against them (and exercise their right to judicial review) if they are prevented from knowing what the allegations actually are.[56] The terrorist listing regime has been described by the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism as a system reminiscent of Franz Kafka's The Trial, whose protagonist 'Josef K., like most of those who are blacklisted, never received a trial' but who faced the same 'combination of procedural limbo and interference with ordinary life that faces those who are blacklisted as suspected terrorists'.[57]

---

[51] *ibid.*, p. 11
[52] Hayes, Ben, 'Time to rethink terrorist blacklisting' in *Statewatch,* Vol. 20 no. ¾, July-December 2010 [online] accessed August 2011, available at http://database.statewatch.org/article.asp?aid=30435
[53] *ibid.*
[54] *ibid.*
[55] Summarised from Hayes and Sullivan, *ibid.*, p. 106
[56] ECCHR, *Executive summary - Blacklisted: Targeted sanctions, preemptive security and fundamental rights,* Berlin, December 2010, [online] accessed August 2011, available at http://www.ecchr.org/index.php/publications/articles/blacklisted-targeted-sanctions-preemptive-security-and-fundamental-rights.864.html
[57] Scheinin, Martin, in Sullivan and Hayes, *ibid.*, pp. 4-5

There are a number of key fundamental human rights provisions enshrined in both international law (the 1948 Universal Declaration of Human Rights (UDHR) and the 1966 International Covenant on Civil and Political Rights (ICCPR)) and European law (the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)) which are encroached upon or violated by the terrorism blacklisting regimes:

- Right to a Fair Trial (UDHR Art. 10, ICCPR Art. 14(1) and EDHR Art. 6(1)[58]
  - Right to be Heard
  - Right to be Informed
- Right to Judicial Review/Effective Remedy (UDHR Art. 8, ICCPR Art. 2(3), ECHR Art. 6, Art. 13)
- Right to Property (peremptory norm of international law, ECHR Art.1, Protocol 1)

Both the UN list and independent EU list are relevant to proscription practices in Europe. There are European measures which implement sanctions under the UN list (UNSCR 1267), as well as an autonomous EU list (created under UNSCR 1373).[59] What is more, although there is no judicial review mechanism available under the UN lists, individuals listed under UNSCR 1267 have challenged their listing in European courts.

The original UN list had no judicial safeguards, and thereby failed to provide:

a) for groups and individuals to be informed of their inclusion on the list;
b) for them to know or have access to the allegations against them; or
c) for them to challenge their inclusion on the list, either to the Sanctions Committee (in charge of listing under the UN 1267 list) or to any other independent court or tribunal.[60]

The numerous 'legal challenges (and the political campaigns surrounding them) have been the primary means of bringing about the reform of blacklisting regimes, albeit, in an ad hoc and haltingly incremental manner, and opening spaces for challenging their legitimacy.'[61] Following legal, political and civil pressure, the UN list has undergone some minimal procedural reform, culminating in the 2009 appointment of an Ombudsperson (OP) to facilitate delisting requests. The Ombudsperson however has no decision-making power, no mandate to make recommendations to the Sanctions Committee, and restricted access to information on the reasons for a listing; such access is at the discretion of the State who listed an individual or organisation, and who may or may not choose to disclose their evidence. The reforms to the UN list fail 'to address the fundamental problems running to the core of the blacklisting system: including the lack of judicial review and effective remedy for those on the blacklist and the non-disclosure of the confidential or classified information underpinning the listing decision'.[62]

Like the UN, 'the EU had originally made no provision for notification of the affected parties or introduced procedures for them to be removed from the autonomous list.' Since 2007 however, in response to mounting judicial dissent, there have been some substantive procedural reforms of the EU list. In June 2007, several reforms were introduced, including;

- A formal EU sanctions committee;
- Notification and provision of a statement of reasons to all those listed;

[58] For more details, see Ch.3, 'Blacklisting and Human Rights' in Sullivan and Hayes, *ibid.,* pp. 26-40
[59] For more details on how the EU lists are established and on what legal basis, see Sullivan and Hayes, *ibid.,* p. 17
[60] Summarised from Sullivan and Hayes, *ibid.,* p. 14
[61] Scheinin, Martin, in Sullivan and Hayes, *ibid.,* p. 42
[62] Sullivan and Hayes, *ibid.,* pp. 108-109

- A six-month review procedure of the EU blacklist;
- A 'focal point' for delisting applications.

One of the most significant legal cases that led to reform was that of Yassin Abdullah Kadi, who successfully challenged the European implementation of his UN listing in the European Court of Justice (ECJ). In 2008 the ECJ ruled that despite the supremacy of the United Nations in the hierarchy of international law, the principle of due process enshrined in the European Convention on Human Rights had to take priority.[63] This case led to a shift from 'automatic compliance' to 'controlled compliance' whereby the European institutions can no longer simply automatically implement the UN 1267 list but must first consider (and retrospectively consider for those on the existing list) whether the European implementation of the list is compatible with fundamental rights.[64]

These reforms have however been rejected by the European courts (including various Member State courts and the European Court of Justice) as sufficient to uphold fundamental rights. The 'controlled compliance' system means that 'the European Commission are to explicitly take the views of blacklisted individuals and groups into consideration before exercising their own discretion as to whether they should be designated on the European lists,'[65] but the General Court has found that this right to defence is being observed in only the 'most formal and superficial sense'. The Commission neither took Kadi's defence as a reason to call into question the findings of the Sanctions Committee, nor did they grant him 'even the most minimal access to the evidence against him'.[66] Thus, the continuation of the Kadi case, and the 'controlled compliance' method it embodies, demonstrates that the right to defence and to effective judicial review is still being denied.[67] Without the disclosure of the key material underpinning a listing decision, it is impossible to effectively exercise the right of review before the European courts, which leaves that right largely without substance.

Whilst the EU provides a relatively higher standard of 'due process' than the UN, its blacklisting regime still falls far short its substantive obligations to introduce a much fairer system that respects both fundamental rights and the principles of proportionality and democratic control.[68] What is more, the EU and its Member States:

> *"must take their share of responsibility for the failure to resolve the crisis of the blacklists at the level of the United Nations. It is simply unacceptable for EU officials to continue to complain privately that they wish the UN had not saddled the European judicial system with the 'burden' of a glut of human rights and due process cases while failing to press the UN to engage in the meaningful reform so clearly demanded by its own Courts."*[69]

There are broader implications of blacklisting policies, above and beyond the effects on individuals who have been listed. These include:

- the expansion of the executive powers of governments
- the expansion of the executive powers of the UN Security Council (the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental

[63] Summarised from Sullivan and Hayes, *ibid.,* pp. 57-61
[64] Summarised from Sullivan and Hayes, ibid., p. 17
[65] Sullivan and Hayes, *ibid.,* p. 110. This includes retrospective consideration for those on already on the list.
[66] *ibid.*, pp.110-111
[67] Summarised from *ibid.*, pp. 110-111
[68] This is noted in Hayes, *ibid.*
[69] Sullivan and Hayes, *ibid.,* pp. 126-127

Freedoms While Countering Terrorism concluded in a formal report that this goes beyond the legal powers conferred upon them by Ch VII of the UN Charter)[70]
- the use of administrative rather than criminal law weakening the judicial and democratic control of executive powers;
- the legitimization of pre-emptive action;
- the outsourcing of the definition of terrorism enabling repressive governments to criminalise political opponents by branding them terrorists;
- potentially undermining the right to self-determination; and,
- the gendered impacts of terrorist listing (women have been shown to disproportionately bear the brunt of measures like asset-freezing, reporting obligations, etc.)[71]

One of the most serious concerns for QCEA is the way in which the EU's 'autonomous listing regime is criminalising resistance movements [and] paralysing peace processes.'[72] Terrorist lists, by placing individuals and organizations under political and economic sanctions can adversely affect attempts at mediation, conflict-prevention and resolution, and peacebuilding, by:

- **Preventing states from even undertaking negotiations with key non-state actors involved in conflicts**. For example, the Norwegian government's position in various international peace negotiations, including between the Sri Lankan state and the LTTE (Liberation Tigers of Tamil Eelam) who are listed, led it, in 2006, to withdraw all support from EU terrorist list, because it would 'cause difficulties for Norway in its role as neutral facilitator in certain peace processes. Norway's role could become difficult if one of the parties involved was included on the EU list, and the opportunities for contact were thus restricted'.[73] Similarly, an EU diplomatic delegation who visited the Middle East in January 2009, in an attempt to negotiate a ceasefire between Israel and the Gaza Strip, did not meet with Hamas (who govern the Gaza Strip), as both its political and military divisions have been listed since at least 2002, despite objections from both France and Germany that such designation would hamper peace efforts in the region. The delegation, when asked why they had not met with one of the key protagonists of the conflict they were seeking to resolve during a self-stated peace mission, simply said 'Hamas is on this list of terrorist organisations and this is the policy we are applying because it has been decided unanimously by the European Union.'[74]
- **Antagonising negotiating parties and / or providing them with rhetorical legitimacy to resort to the use of force**. The EU's listing of LTTE is generally accepted to have played a clear and tangible role in undermining the Sri Lankan peace process facilitated by the Norwegian government. Despite the acknowledgement that increasing violence was not the LTTE's responsibility alone, with a growing number of extrajudicial killings, once the LTTE were listed by the EU they demanded the departure of the international monitors (from Denmark, Finland and Sweden) 'who had been monitoring the ceasefire agreement of 2002, stating that "European Union ban on the LTTE has seriously disturbed" the neutrality of these countries, and they would therefore have to be replaced. In addition to disrupting the peace process, observers argued that the EU listing itself effectively gave "carte blanche" for the Sri Lankan government to seek a military solution to the conflict'.[75]

Today, most armed conflicts are asymmetrical, 'opposing internationally legitimized state actors against non-state armed groups – often labelled or legally proscribed as "terrorist

[70] This is noted in Sullivan and Hayes, *ibid.,* p. 105
[71] This list is summarised from Ch 5 'Broader Impacts of the Lists' in Sullivan and Hayes, *ibid.,* pp. 78-99
[72] Sullivan and Hayes, *ibid.,* p. 127
[73] *ibid.* p. 90
[74] *ibid.* pp. 90-91
[75] *ibid.* p. 91

organizations".'[76] The demands of conflict transformation in such contexts mean that any successful peacebuilding attempt requires:

> *"the engagement of all main conflict stakeholders; in particular, armed groups representing large social or ethnic constituencies with legitimate collective grievances and who possess the capacity to either impede or facilitate constructive social change must be involved in conflict settlements."*[77]

What is more, peace talks require a certain parity of status and good faith – the official legitimizing / delegitimizing of terrorist listing can antagonize protagonists and catalyze the use of force, tending to further deepen the level of mistrust, especially where conditions and incentives for delisting are not clearly indicated.

Many non-governmental organizations (NGOs) engage in peacebuilding activities, for example, training and capacity building (such as teaching groups about federalism, power sharing, interim arrangements, etc.), which can be a precondition for peace negotiation processes in highly asymmetric conflicts. Inclusion of a group on a list may mean that capacity building for that group is seen as a form of material support and therefore illegal. For example, the conflict transformation activities conducted by the German NGO Berghof Peace Support and Berghof Conflict Research, which include capacity-building and mediation and negotiation support (for example, with the LTTE), have been subject to the regulations of the EU list, leading to difficulties in terms of venues, visa, donor restrictions and other political sensitivities.[78]

Blacklisting and financial sanctions rules have also impacted on charitable giving and international money transfers, in a way that can hinder legitimate work in development, relief or peacebuilding, in conflict zones or areas associated with terrorist activity. Non-profit organizations (NPOs) 'regularly support efforts in the field by reaching populations who are vulnerable or susceptible to criminals' interests. Undue suspicion should therefore not be cast upon NPOs that are active -- in some cases with government funds -- in regions where terrorist organisations are known to be active, nor should additional reporting burdens be required'.[79]

> *"On the one hand [NPOs] have had to adjust to the due diligence obligations imposed by EU law, on the other they have found their work in conflict zones and fragile states paralysed by the blacklisting of groups and individuals with whom they had previously been in contact (for example as part of conflict resolution or peace-building activities)"*[80]

More broadly, the suspicion which falls onto NPOs working in areas where listed organizations are suspected to be active, also falls onto the wider communities associated with whatever cause a listed organization may uphold. Yet many people who may sympathise with the cause, may at the same time not support terrorist or violent activities at all. This creation of 'suspect communities' has cast Muslims, Tamils, Palestinians or Kurds who live in Europe as potential members or supporters of terrorist organizations. Solidarity

[76] Wils, Oliver and Dudouet, Véronique, *Peace Mediation and Listed Terrorist Organizations: Challenges for Peacebuilding. Some Thoughts based on the experience of the Berghof Institutions*, June 2010, [online] accessed October 2011, available at http://www.berghof-peacesupport.org/publications/RLM_Peace_Mediation_and_Listed_Terrorist_Organizations.pdf
[77] *ibid.*
[78] This and the previous paragraph have been summarised from *ibid.*
[79] EFC/CORDAID/SBF, *Joint comments on the discussion paper: "Voluntary guidelines for EU based non-profit organizations",* 10th September 2010, [online] accessed October 2011, available at http://www.efc.be/EUAdvocacy/EFC%20Statements/2010_EFC_CordaidJoint-SBF-comment_10September.pdf
[80] Sullivan and Hayes, *ibid.,* p. 89

with a cause or a plight of a people is not and should not be understood to be the same as 'encouraging or engaging in violent acts on behalf of that cause'.[81] Similarly, financial donations to Islamic charities should not automatically ring alarm bells or raise suspicions of NPOs being used for or shielding terrorist financing, given that charitable giving is one of the five pillars of Islam and a religious obligation for Muslims. Suspicion and stigmatization of such communities does nothing to help assuage the root causes of terrorism.[82]

The European Centre for Constitutional and Human Rights (ECCHR) observes that:

a) Neither an independent review mechanism at UN level, nor review of UN blacklists at national level are likely to be acceptable to the UN Security Council;
b) The security interests of states are directly at odds with the disclosure of information on 'suspects';
c) Disclosure is a precondition for effective review;
d) The UN blacklisting system has suffered increasing undermining of its legality and legitimacy (e.g. by the ECJ's ruling);
e) There are inherent problems which result from a lack of an internally accepted definition of terrorism brings.

Because of all these concerns, the ECCHR recommends that *the UN blacklisting regime (UNSCR 1267 and 1373, including the EU list which came out of UNSCR 1373) be abolished, and replaced with a different solution.*[83]

QCEA echoes these concerns and the recommendations that flow from them.

The UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism has recommended that:

> *"The Security Council should seize the opportunity of the approaching tenth anniversary of its resolution 1373 (2001) to replace resolutions 1373 (2001), 1624 (2005) and 1267 (1999) (as amended) with a single resolution not adopted under Chapter VII of the Charter of the United Nations … Chapter VII does not provide the proper legal basis for maintaining the current framework of mandatory and permanent Security Council resolutions of a quasi-legislative or quasi-judicial nature."*[84]

This recommendation is based on the arguable ***unlawfulness*** of the listing/sanctions regime, the ***ineffectiveness*** of the regime in meeting its ostensible goal of promoting international peace and security by blocking terrorist finance, and the systematic and serious ***undermining of fundamental rights***.[85] The adverse effects on conflict resolution and peace-building are also a key concern, which indicates the continued need to work towards a clear and precise international definition of terrorism and terrorist acts, and the necessary links between individual/entity and act, in order to avoid politically or ideologically motivated designations, which can serve to criminalise or demonise one side of an asymmetrical conflict (or perceived supporters thereof) between state and non-state actors who both may share legitimate grievances and who both may hold responsibility for unlawful acts of violence.

[81] *ibid.,* p. 88
[82] Summarised from *ibid.,* p. 89
[83] Summarised from *ibid.*
[84] UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism in Sullivan and Hayes, *ibid.,* p. 117
[85] Summarised from Sullivan and Hayes, *ibid.,* pp. 117-118

The abolition of the UN blacklisting regime would remove the legal requirement for the EU list and therefore open the way for a much needed broader public debate on EU terrorist lists and human rights violations, and the compatibility of placing those who have neither been convicted nor are awaiting trial for terrorist offences, with the values upon which the EU is founded. Although the European Parliament has been, since the Lisbon Treaty, quite vocal on aspects of counter-terrorism policy, from the Passenger Name Record to the Terrorist Finance Tracking Programme, they have yet to engage significantly with the issue of terrorist listing. This should be remedied, so that the terrorist listing regime in Europe gets the kind of scrutiny and democratic accountability it deserves. This kind of pre-emptive, control-based response to the threat of terrorism represents, at best, an inflexible and regressive response to a perceived emergency, but at worst, a system of guilty until proven innocent, which at the same time precludes the very possibility of proving one's innocence.

5. Extraordinary Rendition, Secret Detention and Complicity in the Use of Torture

> *"The fact that European states colluded in such egregious violations – illegal transfers, secret detention, and torture and ill-treatment; crimes under international law, in fact – is sobering."* – Amnesty International[86]

The Council of Europe (CoE) initiated an investigation in 2005, led by Dick Marty, into the alleged illegal CIA secret prisons in Europe, to ascertain whether the "rendition" of terror suspects for possible torture, or illegal secret detentions, had taken place in any of the CoE's 47 member states, as part of the US "war on terror" since 2001. A report released in 2006, following the examination of aviation logs, satellite images and numerous other sources of information, concluded that fourteen European countries had participated in the perpetration of such abuses.[87](See Figure 1).

A second CoE report in 2007, noted that:

> *"What was previously just a set of allegations is now proven: large numbers of people have been abducted from various locations across the world and transferred to countries where they have been persecuted and where it is known that torture is common practice. Others have been held in arbitrary detention, without any precise charges levelled against them and without any judicial oversight – denied the possibility of defending themselves. Still others have simply disappeared for indefinite periods and have been held in secret prisons, including in member states of the Council of Europe, the existence and operations of which have been concealed ever since."*[88]

[86] Amnesty International, *Open secret: Mounting evidence of Europe's complicity in rendition and secret detention,* 2010, p. 38 [online] accessed August 2011, available at http://www.amnesty.org/en/library/asset/EUR01/023/2010/en/3a3fdac5-08da-4dfc-9f94-afa8b83c6848/eur010232010en.pdf

[87] Marty, Dick, *Alleged secret detentions and unlawful inter-state transfers of detainees involving Council of Europe member states,* Doc. 10957, Council of Europe Report, Committee on Legal Affairs and Human Rights, 12 June 2006, [online] accessed August 2011, available at http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc06/EDOC10957.htm

[88] Marty, Dick, *Secret detentions and illegal transfers of detainees involving Council of Europe member states: second report, Explanatory memorandum,* Council of Europe Report, Committee on Legal Affairs and Human Rights, 7 June 2007, [online] accessed August 2011, available at http://assembly.coe.int/CommitteeDocs/2007/EMarty_20070608_NoEmbargo.pdf

The CoE has reaffirmed 'its absolute commitment to overcoming the threat of terrorism' but that stated that it 'must equally speak out in the strongest possible terms against the numerous and systematic human rights abuses committed in the pursuit of the so-called "war on terrorism"… such violations play into the hands of the terrorists and ultimately serve to strengthen those who aim to destroy the established political, legal and social order.'[89]

Figure 1.

90

It is for this reason that it is not only morally unacceptable, but thoroughly counter-productive, that the US, in their post-9/11 attempts to address the terrorist threat, rejected both the instruments of criminal law and procedure, and the framework of the laws of war (including respect for the Geneva Conventions) and instead introduced previously unheard of 'legal' concepts, such as 'enemy combatant' and 'rendition', which are contrary to basic legal principles and fundamental rights.[91] This has led to 'a world-wide network of secret detentions on CIA "black sites" in military or naval installations; the CIA's programme of "renditions", under which terrorist suspects are flown between States on civilian aircraft, outside of the scope of any legal protections, often to be handed over to States who customarily resort to degrading treatment and torture; and the use of military airbases and aircraft to transport detainees as human cargo to Guantanamo Bay in Cuba or to other detention centres.'[92] It is the fact that some EU and CoE Member States have been complicit in these actions that is of direct concern here.

[89] Marty 2006, *ibid.* p. 2
[90] Source of map: Amnesty International, *ibid.*
[91] Summarised from Marty 2006, *ibid.* p. 2
[92] Marty 2006, *ibid.* p. 2

Without attempting to be exhaustive, when it comes to which European countries have been implicated in what, it can be noted that:

- According to the CoE, there is sufficient evidence to state that 'secret detention facilities run by the CIA did exist in Europe from 2003 to 2005, in particular in Poland and Romania' hosted 'under a special CIA programme established by the American administration in the aftermath of 11 September 2001 to "kill, capture and detain" terrorist suspects deemed to be of "high value."'[93]
- The UN Special Rapporteurs on Torture and on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism have also concluded, in a joint February 2010 report, that 'Germany (one case, 2002) and the UK (several cases, from 2002 onward) had been complicit in secret detentions of terrorism suspects.'[94]
- The CoE Commissioner for Human Rights, in June 2010, criticized the 'lack of progress towards full accountability for complicity in United States abuses in Poland, Romania, and Sweden.'[95]
- In Lithuania, following the conclusions of a parliamentary committee 'that the CIA had established two secret detention facilities in that country in 2005 and 2006', a criminal investigation was launched in January 2010.[96]
- Aircraft chartered by the CIA for the purpose of carrying 'terrorism suspects to locations around the world, where they were often tortured'[97] have been revealed to have 'frequently passed through British and Irish airports en route, including Shannon, Glasgow, Edinburgh and London Luton'.[98] The same documents revealed that CIA chartered aircraft flew 'direct from a European airport to Guantánamo.'[99]

The CoE have concluded that evidence has demonstrated that 'the CIA committed a whole series of illegal acts in Europe by abducting individuals, detaining them in secret locations and subjecting them to interrogation techniques tantamount to torture. In most cases, the acts took place with the requisite permissions, protections or active assistance of government agencies.'[100] On a positive note, Amnesty International has noted that 'some notable progress toward accountability for European governments' roles in the CIA-operated rendition and secret detention programmes' has been made, albeit 'without the co-operation of the US government and in some cases, in spite of the lack of political will and outright obstruction by some European governments.' They note that 'inquiries into state complicity or legal processes aimed at individual criminal responsibility have occurred, or are currently in process' in Germany, Italy, Lithuania, Macedonia, Poland, Romania, Sweden, and the United Kingdom.[101]

This progress (which varies in degree in these different countries) toward proper investigation into complicity, has been obstructed by some governments who invoke the concept of "state secrets", notably Germany and Italy.[102] The CoE have stated that 'neither national security nor state secrecy can be invoked in such a sweeping, systematic fashion as to shield these unlawful operations from robust parliamentary and judicial scrutiny.'[103]

---

[93] Marty 2007, *ibid.* p. 4
[94] Human Rights Watch (HRW), *World Report 2011: European Union - Events of 2010*, [online] accessed August 2011, available at http://www.hrw.org/en/world-report-2011/european-union#_Counterterrorism_Measures_and
[95] *ibid.*
[96] *ibid.*
[97] Cobain, Ian and Quinn, Ben, 'How US firms profited from torture flights' in *the Guardian*, 31 August 2011, [online] accessed August 2011, available at http://www.guardian.co.uk/world/2011/aug/31/us-firms-torture-flights-rendition
[98] Reprieve, *Huge stash of rendition documents reveal how the CIA covered its tracks*, 31 August 2011, [online] accessed August 2011, available at http://www.reprieve.org.uk/press/2011_08_31_rendition_documents/
[99] Cobain and Quinn, *ibid.*
[100] Marty 2007, *ibid*. p. 5
[101] Amnesty International, *ibid.* p. 5
[102] For more information, see Marty 2007, *ibid.* p. 3
[103] Marty 2007, *ibid.* p. 3

Indeed, invoking state secrecy, even years after the event, is at odds with the workings of a democratic state based on the rule of law, and the CoE have noted that 'state secrets are invoked on grounds almost identical to those advanced by the authorities in the Russian Federation in its crackdown on scientists, journalists and lawyers, many of whom have been prosecuted and sentenced for alleged acts of espionage.'[104] With regard to this threat to accountability, justice and redress, Amnesty International has urged that:

> *"Europe, however, must not become yet another "accountability-free zone", with governments eager and enabled simply to forget the past or to whitewash inquiries into their involvement in these egregious practices. If such collective amnesia or exoneration by perfunctory investigation is not challenged, Europe will be complicit in a profoundly damaging overarching violation of international law in relation to what the USA previously called the "war on terror": creating an environment of impunity for grave human rights violations and denying victims the redress to which they are so clearly entitled. Any such impunity would constitute a serious failure to respect international human rights law, with the ripple effect of undermining efforts to encourage respect for human rights by governments elsewhere in the world."*[105]

Calls for systematic, thorough and independent investigation have come not only from Amnesty International and other human rights organizations, but from the Council of Europe and the European Parliament. The CoE noted that as it has been demonstrated incontestably that European countries have been involved in secret detentions and unlawful interstate transfers, there is a requirement for 'in-depth inquiries and urgent responses by the executive and legislative branches of all the countries concerned.'[106] Moreover, the authorities concerned must 'stop obstructing the efforts under way in judicial and parliamentary bodies to establish the truth' and serious consideration must be given 'to ways of avoiding similar abuses in future and ensuring compliance with the formal and binding commitments which states have entered into in terms of the protection of human rights and human dignity.'[107]

The European Parliament has also been vocal on these issues, and has stated that 'the complicity by several European governments that has been ascertained by the European Parliament's investigation into the "extraordinary rendition" of terrorist suspects by the CIA to their home countries as a manner of subcontracting torture in order to obtain information, is equivalent to legitimising these practices.'[108] A parliamentary resolution in February 2009 called on the EU, Member States, and US authorities:

> *"to investigate and provide full clarification about the abuses and violations of international and national law on human rights, fundamental freedoms, the prohibition of torture and ill-treatment, enforced disappearance and the right to a fair trial committed in connection with the 'war against terror', so as to establish responsibility for secret detention centres - including Guantánamo - and the extraordinary rendition programme, and to ensure that such violations will not recur in the future and that the fight against terrorism is pursued without breaching human rights, fundamental freedoms, democracy and the rule of law;"*[109]

---

[104] Marty 2007, *ibid.* p. 3
[105] Amnesty International, *ibid.* p. 6
[106] Marty 2006, *ibid*. p. 3
[107] Marty 2007, *ibid.* p. 5
[108] Maccanico, Yasha 'The effects of security policies on rights and liberties in the European Union, and their export beyond the EU's borders' in *Statewatch Analysis,* May 2011 [online] accessed August 2011, available at http://www.statewatch.org/analyses/no-128-sec-lib-eu.pdf
[109] Official Journal of the European Union, *European Parliament resolution of 19 February 2009 on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners,* 2010/C 76 E/11, [online] accessed August 2011, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:076E:0051:0054:EN:PDF

Despite some progress in this area, a full investigation has still not been carried out to a sufficient degree, at either EU level or (systematically) at Member State level, and as recently as July 2011, the Parliament stated that *'The EU and its Member States must fully clarify their role in the CIA programme of renditions, in the light of new evidence brought to light thereafter… the EU must help the US to find appropriate was to close the Guantánamo detention facility and ensure that its prisoners get a fair trial.'*[110]

Following a decade of smoke and mirrors surrounding the absence of due process or remedy, breaches to the absolute prohibition of torture, and high-level impunity regarding these matters, it can be said that 'the legal obligation to look back and ensure full accountability for such violations has been ignored by these governments for too long.'[111] To be quite clear, 'international law leaves no place to hide for European states that are legally responsible for their part in facilitating renditions and secret detention.' What is more, 'in order to ensure that such abuses do not occur in the future, European governments must implement reforms for the civilian oversight of national intelligence and security agencies and of foreign intelligence agencies operating on their territories.' [112]

QCEA adds its unequivocal support to ensure that EU and CoE Member States fully carry out the recommendations of the Council of Europe, the European Parliament, and the numerous human rights organizations that have campaigned tirelessly get these issues into the limelight.[113]

6. The Internet and Counter-terrorism

The internet is relevant to the area of counter-terrorism in two main ways – concerns over cyber security, and the misuse of the internet for violent radicalization and recruitment into terrorism. Cyber security 'means protection of our vital infrastructures (state and private communication) against attacks in cyber space.'[114] This has become an area of increased concern, under the Protect strand of CT policy, and according to the CTC, whilst 'cyber terrorism is not the major hazard', cyber attacks may be attractive to terrorists as they are 'a cheap tool, targets can be attacked from all around the world, a small attack can have a huge impact, and the internet still offers anonymity', and therefore, 'we have to start our preparation before terrorists acquire know-how or capacities to target our infrastructures'.[115] Developing plans in this area will certainly need to be kept under scrutiny.[116]

Our current major concern relates to how violent radicalization aided by the internet is being dealt with, and the consequent methods of intelligence gathering for counter-terrorism intelligence purposes.

---

[110] Civil Liberties, Justice and Home Affairs Committee, *Counter-terrorism policy needs proper evaluation, says Civil Liberties Committee.* Press Release, 13 July 2011, [online] accessed August 2011, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20110711IPR23776+0+DOC+XML+V0//EN&language=EN

[111] Amnesty International, *ibid.* p. 5

[112] *ibid.* p. 6

[113] Including but not limited to Amnesty International, Reprieve, Statewatch and Human Rights Watch.

[114] Counter-terrorism coordinator, *Note from EU Counter-Terrorism Coordinator to Council / European Council on EU Counter-Terrorism Strategy - Discussion paper*, 15894/1/10 REV 1, Brussels, 29 November 2010, p. 7 [online] accessed August 2011, available at http://www.consilium.europa.eu/uedocs/cmsUpload/st15894-re01%20en10.pdf

[115] *ibid*. p. 6

[116] For more details on the future plans of the EU in the area of cyber-security, see *ibid.* pp. 6-8

Part of the Prevent strand on EU CTC strategy is the 'Check the Web' (CTW) work stream 'where Member States work to strengthen the monitoring of militant Islamic websites'.[117] The Commission has also started a public/private partnership approach for countering terrorist use of the internet. Reputedly, a European Agreement Model to facilitate public/private cooperation on the issue is under development, as well as 'a dialogue between law enforcement authorities and service providers to reduce the dissemination of illegal terrorism-related content on the internet.'[118]

The use of systematically collected, processed and analysed data from the internet - which is 'public' in so far as it is not classified 'confidential', 'private' or otherwise 'intended for or restricted to a particular person, group or organization' - is not, on the face of it, problematic. However, the categorisation of 'weblogs', internet 'chat-rooms' and social-networking sites as "public speaking forums", combined with the powers being assumed by private companies in profiling and selling this data, are cause for concern.[119] Concerns about the use of the internet for terrorist propaganda are legitimate, but so too are the worries about EU sanctioned use of '[p]rivate companies free from the privacy statutes that constrain state agencies [who] are collecting data on a vast scale'.[120] Moreover, there is a distinction between radicalization of beliefs and violent radicalization (with the intent to commit or incite violent action), but this distinction is largely ignored.

Open Source Intelligence (OSINT) is 'information derived from publicly accessible sources (media, books, reports, conferences, the Internet etc). It is not a new discipline, but it has received an incredible boost from the rapid growth in information available online via the Internet.'[121] The EU systematically uses OSINT, via both public and private sector means, in the fight against violent radicalization and recruitment to terrorism, and has recognised that 'novel techniques and tools are becoming increasingly necessary to harvest new data sources such as Blogs, Twitter and other social media systems.'[122] Moreover, the need to take advantage of this so-called 'digital tsunami' in security-oriented areas is seen as key, because '[e]very object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts.'[123] More sinisterly put, the internet can be considered an Orwellian dream;

> *"the nearest thing to a perfect surveillance machine the world has ever seen. Everything you do on the net is logged – every email you send, every website you visit, every file you download, every search you conduct is recorded and filed somewhere, either on the servers of your internet service provider or of the cloud services that you access. As a tool for a totalitarian government interested in the behaviour, social activities and thought-process of its subjects, the internet is just about perfect."*[124]

[117] Counter-terrorism coordinator (CTC), *Note from EU Counter-Terrorism Coordinator to Council / European Council on EU Action Plan on combating terrorism,* 15893/1/10 REV 1, Brussels, 17 January 2011, p. 5 [online] accessed July 2011, available at http://register.consilium.europa.eu/pdf/en/10/st15/st15893-re01.en10.pdf
[118] *ibid.*, pp. 5-6
[119] Paraphrased from Hayes, Ben, 'Spying in a see through world: the "Open Source" intelligence industry' in *Statewatch Journal*, Vol. 20, No. 1, January-March 2010, [online] accessed August 2011, available at http://www.statewatch.org/analyses/no-119-open-source-intell-industry.pdf
[120] *ibid.*
[121] European Defence Agency, *Open Source Intelligence*, [online] accessed August 2011, available at http://www.eda.europa.eu/Otheractivities/Intelligence/Training/Opensourceintelligence
[122] European Commission Joint Research Centre, *Open Source Text Information Mining and Analysis (OPTIMA),* Action number 31006; details can be found [online] accessed August 2011, available at http://projects.jrc.ec.europa.eu/jpb_public/act/publicexportworkprogramme.html?actId=240&d-2325611-p=5
[123] Maccanico 2011, *ibid.*
[124] Naughton, John, 'The internet: Everything you ever need to know', in *the Observer,* 20th June 2010 [online] accessed August 2011, available at http://www.guardian.co.uk/technology/2010/jun/20/internet-everything-need-to-know

On the one hand, from a security intelligence perspective, it is surely true that 'security services would be negligent if they did not utilise information in the public domain to inform their work; everyone else engaged in public policy matters does the same thing.'[125] Indeed, the 'CIA has even been quoted as saying that "80% of its intelligence comes from Google."'[126] On the other hand, from a civil liberties perspective, 'the process of appropriating personal information for the purpose of security classification *is* inherently problematic, since it is often based on wholly flawed assumptions about who or what poses a 'threat'. The mere act of recording that someone spoke out publicly against the war, attended a demonstration, or is friends with a known 'security risk', brings with it a significant possibility that this information will be used prejudicially against them at some point in the future. This in turn calls into question the democratic legitimacy of surveillance and intelligence gathering, a legitimacy that rests on questions of who is doing the watching, how, and why?'[127]

It is the privatization of intelligence that is especially problematic in this respect, because whilst OSINT collection may be done efficiently by private sector research institutes and companies,[128] as well as potentially relieving budgetary pressures, when it comes to the privacy statutes that 'constrain governments' ability to collect information on citizens who are not the targets of actual police' investigations, "law enforcement agencies are increasingly circumventing that requirement by simply purchasing information that has been collected by data aggregators."'[129] The legal right to privacy and to non-discrimination are enshrined in European law, yet these private companies conduct data aggregation, risk intelligence gathering and explicitly engage in profiling people. For example, World-Check states on its website that it 'methodically profiles individuals and entities deemed worthy of enhanced scrutiny.'[130]

Whilst much OSINT collection is simply mining publically available sources, there has also been a huge development of 'spyware' applications, which enable users to conduct covert and intrusive surveillance, including:

> *"'phishing' applications, used to acquire sensitive information such as usernames and passwords, and a variety of 'keystroke loggers', used to surreptitiously record computer users activities… Although the EU has criminalised the unauthorised use of spy-ware, hacking and interception techniques, this has done nothing to stem their development. Moreover, some EU law enforcement are clearly using them, having repeatedly demanded so-called 'lawful access' powers, allowing them to legally access suspects' computer hard drives through the internet, and without the knowledge of those affected. The crux of the matter is that both the police and the private investigator are steadily accumulating the capacity (if not the lawful powers) to conduct the kind of covert and intrusive surveillance that was once the preserve of GCHQ [government communications headquarters] and the secret intelligence services."*[131]

[125] Hayes, Ben, 'Spying in a see through world: the "Open Source" intelligence industry' *ibid.* p. 2
[126] *ibid.* p. 2
[127] *ibid.* p. 2
[128] There are a number of private companies engaged in what is now an industry worth billions, including *Acxiom*, *Choicepoint*, *Lexis-Nexis, Equifax, Experian, World-Check, Infosphere AB, Sandstone AB, RAND Corporation, Jane's, Factiva, Oxford Analytica, CEIS-Europe, Columba Global Systems*. Research institutes include the University of Southern Denmark's Counterterrorism Research Lab, who conduct research and development around '*advanced mathematical models, novel techniques and algorithms, and useful software tools to assist analysts in harvesting, filtering, storing, managing, analyzing, structuring, mining, interpreting, and visualizing terrorist information'- ibid.* pp. 3-7
[129] *ibid.* pp. 3-4
[130] *ibid.* p. 4
[131] *ibid.* p. 6

In 2006, the EUROSINT Forum, a Belgian not-for-profit association "dedicated to European cooperation and use of [OSINT] that prevent risks and threats to peace and security" was launched, with the support of the European Commission's then Justice, Liberty and Security (JLS) Directorate, the backing of the EU Joint Situation Centre (SITCEN) and support from the EU Security Research Programme (ESRP). Their main aim is the promotion of public-private sector cooperation in the use of OSINT, and its members include 'EU institutions, national defence, security and intelligence agencies, private sector providers of intelligence, technology developers, universities, think-tanks and research institutes.'[132] The EU Joint Research Centre (JRC) has even developed its own OSINT tools for web mining and information extraction, 'to identify *potentially* dangerous people by analysing information on the web, techniques that are coming to be known as counter-radicalisation.'[133]

Other projects funded by the ESRP include SAFIRE (Commission contribution of €3 million) which promises a 'Scientific Approach to Fighting Radical Extremism' and has the goal of 'improv[ing] fundamental understanding of radicalization processes and us[ing] this knowledge to develop principles to improve (the implementation) of interventions designed to prevent, halt and reverse radicalization.'[134] The SAFIRE consortium comprises the Dutch military research institute *TNO,* the *RAND Corporation*, Israel's *International Counter-Terrorism Academy* and *CEIS*. This is all part of the "Prevent" strand of EU CT policy, and as mentioned above, the action plan for radicalisation and recruitment to terrorism. Aside from the concerns about the loss of privacy and data protection through public-private sector cooperation however, the expansion of this programme to tacitly include political activists from across the political spectrum is another distinctly foreboding development.

The Council Conclusions of 26 April 2010 called for the use of a 'standardised, multidimensional semi-structured instrument for collecting data and information on the processes of radicalisation in the EU.'[135] Whilst analysing the various environments where radicalisation occurs and introducing systematic ways of exchanging information on individuals or groups who use hate speech or incite terrorism, with a view to 'interrupt radicalization processes in progress or to raise alerts in relation to them'[136] ('alerts' could trigger action, such as questioning, placing under surveillance, detention, etc.) appears, on the face of it, to be a logical step for the EU to take, Statewatch has raised concerns about the details of the plan. They express concern over the equivocation between the use of the terms 'violent radicalisation' and 'radicalisation', as if they were synonymous. As they note, there are 'millions of people in the EU with "radical" ideas (in the eyes of the state) who may easily, in their own terms, use arguments which are also used by so-called RMs [radical messages] without any intention whatsoever of using or encouraging violence'.[137] The scope of such an instrument has been defined to include extreme right/left, Islamist, nationalist, anti-globalisation etc., where the latter is a vague and catch-all term 'covering just about every group that is opposed to the status quo.'[138] The worry is that any and all 'radicals', be they with intent to use violence or abhor its use, could be indiscriminately targeted, thereby threatening 'open, legitimate political discussion and activity.'[139]

---

[132] *ibid.* p. 7. Member companies (paying the €5,000 EUROSINT annual membership fee) include Jane's, Lexis Nexis, Factiva, Oxford Analytica, CEIS-Europe and Columba Global Systems.
[133] *ibid.* p. 8
[134] *ibid.* p. 8
[135] Council Of The European Union, *ENFOPOL 99*, 8570/10, Brussels, 16 April 2010, [online] accessed August 2011, available at http://www.statewatch.org/news/2010/apr/eu-council-info-gathering-uardicalisation-8570-10.pdf
[136] Bunyan, Tony, 'Intensive surveillance of "violent radicalisation" extended to embrace suspected "radicals" from across the political spectrum, Targets include: "Extreme right/left, Islamist, nationalist, anti-globalisation etc"' in *Statewatch News Online,* May 2010, p. 1-2, [online] accessed August 2011, available at http://www.statewatch.org/analyses/no-98-eu-surveillance-of-radicals.pdf
[137] *ibid.*
[138] *ibid.*
[139] *ibid.*

As summed up by Statewatch, the threat to civil liberties and fundamental freedoms:

> *"comes neither from the internet nor totalitarian governments, but from a neo-McCarthyite witchhunt for 'terrorists' and 'radicals', and a private security industry bent on developing the "perfect surveillance" tools to find them… those of us concerned with freedom and democracy need to see the bigger picture in terms of who is doing the watching, how, and why. We must then develop the tools and communities needed to bring them under democratic control."*[140]

QCEA recommends that any public-private cooperation in this area ensures that the private sector is under as strict non-discrimination and data protection laws as the public sector is, and that the distinction between merely having "radical" beliefs and violent radicalization is clearly defined and effectively upheld. Moreover, the same criticisms and concerns expressed in relation to the Terrorist Finance Tracking Programme and Passenger Name Record are applicable to the blanket surveillance of innocent people on the internet and the profiling activities of private companies.

7. Conclusions and Recommendations

The EU Counter-Terrorism Coordinator (CTC) has recently noted that:

> *"In a number of third countries, human rights and rule of law violations and repression by government agencies in the fight against terrorism are contributing considerably to radicalization. Hence, while these policies are adopted to fight terrorism, in fact they give rise themselves to conditions conducive to the spread of terrorism."*[141]

Having examined some specific policy areas relating to counter-terrorism policy at EU level, it is reasonable to conclude that the CTC's identification of this problem as relating only to third countries is rather optimistic. The EU urgently needs to get its own house in order with respect to human rights and rule of law violations, so as not to undermine its own attempts at minimizing the threat of terrorism.

QCEA recommends that:

- With respect to the Terrorist Finance Tracking Programme (TFTP), QCEA echoes the concerns and recommendations of both the LIBE committee and the EDPS regarding necessity and proportionality, independent oversight and the end to the bulk transfer of data.

- With respect to the Passenger Name Record (PNR), QCEA would reiterate the concerns of the Parliament, the EDPS and Data Protection Working Party, as well as of civil liberties organizations like Statewatch, and urges the Commission and Council to more fully include their recommendations and limitations to PNR, not least the legal opinions presented to the Commission regarding the draft EU-US agreement, as well as more broadly assessing the necessity, and not merely the usefulness, of the instrument. QCEA urges the Parliament to continue exercising its scrutiny and to uphold its commitment to the realization of the fundamental rights enshrined in the Treaties of the EU.

[140] Hayes, 'Spying in a see through world', *ibid.* p. 8
[141] Counter-terrorism coordinator, *Note from EU Counter-Terrorism Coordinator to Council/European Council on EU Counter-Terrorism Strategy - Discussion paper*, 10622/1/11, REV 1, Brussels, 7 June 2011, p.6. [online] accessed August 2011, available at http://register.consilium.europa.eu/pdf/en/11/st10/st10622-re01.en11.pdf

- Regarding both the TFTP and PNR, QCEA notes with caution the encroachment into certain rights and freedoms by instruments whose necessity has not yet been proven, nudging Europe in the direction of a 'surveillance society'. The onus of proof lies on those who claim such instruments are necessary, and they must demonstrate it.

- The UN blacklisting regime (UNSCR 1267 and 1373, including the EU list which came out of UNSCR 1373) should be abolished, and replaced with a different solution that respects fundamental rights to a fair trial, including the right to be heard and to be informed, and the rights to judicial review and effective remedy. As recognized by both the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism and the European Centre for Constitutional and Human Rights, this regime is unlawful, ineffective, systematically undermines fundamental rights and has an adverse effect on conflict resolution and peacebuilding.

- QCEA adds its unequivocal support to ensure that EU and CoE Member States carry out the recommendations of the Council of Europe, the European Parliament, and the numerous human rights organizations who have campaigned tirelessly to get the issues of EU Member States' roles in Extraordinary Rendition, Secret Detention and Complicity in the Use of Torture into the limelight, with respect to systematic, thorough and independent investigation, accountability and appropriate reform.

- QCEA recommends that any public-private cooperation in the use of OSINT ensures that the private sector is under as strict non-discrimination and data protection laws as the public sector is, and that the distinction between merely having "radical" beliefs and violent radicalization is more clearly upheld. Moreover, the trend towards blanket surveillance of masses of innocent people and the profiling of people based on automatic data filtering comes under the same criticisms and concerns expressed in relation to TFTP and PNR.

Written and researched by Rachel Tansey, QCEA Programme Assistant, 2011. Published October 2011