Hard Choices: Increase Counter-Terrorism Surveillance Powers or Risk Further Terrorist Attacks

Presentation by Dr David Lowe, Liverpool John Moores University at UACES Arena Tuesday 2nd June 2015

Hard Choices: Increase Counter-Terrorism Surveillance Powers or Risk Further Terrorist Attacks

The Terrorist Threat to the EU

The civil war in Syria and the inability to control and defend its north western territory by the Iraqi government has allowed a vacuum to exist thereby enabling Islamist groups, in particular Islamic State (formerly Al Qaeda in Iraq (AQI) and also referred to as ISIL) and the Al Qaeda affiliate, Jabhat al-Nusra Front to flourish and become more powerful in the region. These groups do not just pose a threat to the security of the Syrian/Iraqi region, they pose a threat to the security of nations around the world, especially EU Member States, including the UK. The threat is posed on two fronts. Firstly from the number of citizens from nation states outside Syria and Iraq who have gone to those countries to join Islamist terror groups who have become radicalised to such a degree they see their home state as an enemy. In such circumstances these citizens are more likely to plan and carry out terrorist attacks in their home state. The second threat posed by these groups is how their skilful use of social media is used to radicalise EU citizens and influence them to carry out terrorist attacks in their home EU Member State.

Islamic State was originally the group AQI that split from Jabhat al-Nusra Front in 2013. A predominantly Sunni jihadist terror group, in 2014 we witnessed the rise of Islamic State (also known as ISIS or ISIL).[1] Of the mercenaries that have joined Islamic State, in January 2015 it is estimated that up to 600 UK citizens have gone to Syria and Iraq to join Islamic State to fight, and this could be a conservative estimate.[2] This alarming increase in the number of citizens who have gone to Syria and Iraq to fight with Islamic state has led the Rob Wainwright, the director of Europol (the EU's intelligence policing agency that has no

[1] Malcolm Nance (2015) 'The Terrorists of Iraq' Boca Raton: CRC Press, pp.311-312

[2] Douglas Murray 'Our boys in the Islamic State: Britain's export jihad' *The Spectator* 23rd August 2014 retrieved from http://www.spectator.co.uk/features/9293762/the-british-beheaders/ [accessed 12th September 2014]

operation powers whose main role is to co-ordinate an assist EU Member States' policing agencies) to warn of the security gap facing EU poling agencies as they try to monitor online communications of terrorist suspects which is compounded by the fact that by being in Syria and Iraq these suspects are effectively out of reach.[3] More recently Rob Wainwright has given further concerns security and policing agencies face in monitoring electronic communications used by terrorists saying that hidden areas of the Internet and encrypted communications are making it harder to monitor terrorist suspects, adding that Tech forms should consider the impact sophisticated encryption software has on law enforcement. This can range from blogging websites to social media sources such as Twitter where Wainwright revealed that Islamic State is believed to have up to 50,000 different Twitter accounts, tweeting up to 100,000 messages a day.[4]

In the Netherlands in September 2014 three Dutch citizens were arrested on suspicion of recruiting for Islamic State with the Dutch General Intelligence and Security Service calling that support for Islamic State in the Netherlands amounts to a few hundred followers and several sympathisers.[5] The danger of having Islamic State followers, even where there are small numbers, in the EU's Member States was evident in May 2014 when four people were killed at the Jewish Museum in Brussels[6] by an Islamic State militant, Muhdi Nemmouche.[7]

---

[3] N.3

[4] BBC News (2015) 'Europol chief warns on computer encryption' 29th March 2015 retrieved from http://www.bbc.co.uk/news/technology-32087919 [accessed 30th March 2015]

[5] Aljazeera 'Islamic State fears take holds in Netherlands' 5th September 2014 retrieved from http://www.aljazeera.com/indepth/features/2014/09/islamic-state-fears-take-hold-netherlands-201492131426326526.html [accessed 11th September 2014]

[6] BBC News (2014) 'Brussels Jewish Museum killings: Suspect "admits attack"'. 1st June 2014 retrieved from http://www.bbc.co.uk/news/world-europe-27654505 [accessed 11th September 2014]

[7] Kevin Rawlinson 'Jewish museum, shooting suspect is Islamic state torturer' *The Guardian* 6th September 2014 retrieved from http://www.theguardian.com/world/2014/sep/06/jewish-museum-shooting-suspect-islamic-state-torturer-brussels-syria [accessed 11th September 2014]

Mainly due to the threat Islamic State pose, on the 29th August the UK terrorist threat was raised by the UK's Joint Terrorism Analysis Centre from substantial to severe as terrorist attack are now highly likely.[8] The Monday following the raising of the UK's terrorist threat level, the UK Prime Minister, David Cameron announced the UK would introduce a terrorism related measures that included a proposal that airlines be forced to hand over more information about passengers travelling to and from conflict zones.[9] Europol's 2014 T-SAT Report stated that Syria and Turkey are the main destinations of choice for travellers seeking to joined armed terror groups due to the accessibility of their borders to Islamic state gained territory.[10] Europol also report that specific organised facilitation networks are likely to be involved in ensuring a smooth transition into the more radical fighting groups such as Islamic State, as well as other groups such as Jabhat al- Nusra Front citing the example of Sharia4Belgium as one such network.[11] There is no doubt that EU citizens who have travelled to Syria and Iraq to join groups such as Islamic State and Jahbat al-Nusra Front pose a threat to the EU's security both on their return to their home state and in how the groups' use of social media can influence and ultimately radicalise EU citizens to their cause. Islamic State have adopted another tactic in their use of social media regarding the hostages they hold by releasing a series of videos showing a UK citizen they hold hostage, John Cantlie, who has read out messages form Islamic Sate saying they have been misrepresented by Western media and they will present the truth about the group in forthcoming videos.[12] Clearly this is a cynical use of propaganda through the medium of social media as their past actions cannot be misrepresented and neither can the threat they pose.

---

[8] BBC News (2014) 'UK terror threat is raised to "severe"' 29th August 2014 retrieved from http://www.bbc.co.uk/news/uk-28986271 [accessed 11th September 2014]

[9] BBC News 'David Cameron outlines new anti-terror measures to MP's' 1st September 2014 retrieved from http://www.bbc.co.uk/news/uk-29008316 [accessed 11th September 2014]

[10] Europol (2014) TE-SAT 2014: European Union Terrorism Situation and Trend report 2014The Hague: European Police Office, p23

[11] Ibid p.24

[12] BBC News (2014) 'Video of British hostage John Cantlie released' 18th September 2014 retrieved from http://www.bbc.co.uk/news/uk-29258201 [accessed 19th September 2014]

The Threat of Islamic State/Jabhat al-Nusra Front Influenced terrorist attacks in EU Member States: Post Paris 2015 Attacks

On January 7th 2015 Europe received a stark wake-up call as the threat Islamist groups pose to the Continent's sovereign states with the attack on the offices of the French satirical magazine, Charlie Hebdo where twelve people were killed, ten of the staff of the magazine and two police officers who were protecting the building by Cherif and Said Kouachi. These two brothers were French citizens of Algerian descent who were influenced by Al Qaeda,[13] where the Al Qaeda affiliate, Al Qaeda in the Arabian Peninsula (AQAP) claimed responsibility for the attack.[14] On the 8th January 2015 Amedy Coulibaly killed a policewoman and injured another police officer outside a metro station in Paris and on the 9th January he took a number of people hostage in a Jewish Supermarket in Paris, where he killed four of the hostages before the French police stormed the building killing Coulibaly.[15] Both he and the Kouachi brothers were killed by the French police following two respective siege situations.[16]

Paris was not the sole focus of Islamist terrorist activity in Europe during January 2015. In Brussels the Belgian police executed a warrant at premises suspected to be used by an Islamist terrorist cell that contained citizens who had returned from fighting with Islamic State in Syria/Iraq. While two of the suspects were killed by the Belgian police during the raid, five were arrested for terrorist related offence where the terrorist cell's targets were a

[13] Kim Willsher (2015) 'Gunmen attack Paris magazine Charlie Hebdo offices killing at least twelve' *The Guardian* 7th January 2015 retrieved from http://www.theguardian.com/world/2015/jan/07/satirical-french-magazine-charlie-hebdo-attacked-by-gunmen [accessed 22nd January 2015]
[14] Heather Saul (2015) Al Qaeda in Yemen admits responsibility for the Charlie Hebdo attacks and warns west of more tragedies and terror' *The Independent* 14th January 2015 retrieved from http://www.independent.co.uk/news/world/middle-east/alqaeda-in-yemen-admits-responsibility-for-charlie-hebdo-attacks-and-warns-west-of-more-tragedies-and-terror-9976898.html [accessed 22nd January 2015]
[15] Julian Berger (2015) Paris gunman Amedy Coulibaly declared allegiance to Isis' *The Guardian* 12th January 2015 retrieved from http://www.theguardian.com/world/2015/jan/11/paris-gunman-amedy-coulibaly-allegiance-isis [accessed 22nd January 2015]
[16] BBC News (2015) 'Charlie Hebdo hunt: Kouachi brothers killed in assault' 9th January 2015 retrieved from http://www.bbc.co.uk/news/world-europe-30754340 [accessed 22nd January 2015]

Belgian police station and police officers.[17] The investigation led to connections in Greece where the Greek police arrested several people linked to the Belgian terror plot. In addition to this the Greek police were also searching for Abdelhamid Abaaoud, a Brussels resident of Moroccan origin who is believed to be a ringleader of a jihadi cell based in Belgium and who has links to Al Qaeda, possibly the al-Nusra Front.[18] In the same week in January 2015, German police arrested two men in Berlin on suspicion of recruiting individuals to join Islamic State in Syria and for raising finances for the group.[19] During this period a UK citizen, Imran Khawaja was convicted and received a prison sentence at the Old Baily Court in London for preparing acts of terrorism, attending a terrorist training camp in Syria, receiving training there and for possessing firearms. Khawaja had spent six months in Syria fighting with Islamic state and using social media sources faked his own death in an attempt to return to the UK.[20]

From just the terrorist activities and investigations among the EU Member States from the 7th to the 20th January 2015 one can see how real and lethal the terrorist threat to Europe is from international terrorist groups such as Islamic State and al-Nusra Front. As at the time of writing the fact that up to 5,000 EU citizens have travelled to Syria and Iraq to fight alongside these groups, it is submitted that what Europe has witnessed in the last nine months is only the tip of the iceberg. As more of these citizens return to Europe, the potential for attacks will increase and maintaining surveillance on individuals who have been identified as a terrorist risk will add further to the strain EU Member States security services and counter-

[17] BBC News (2015) 'Belgium charges five over terror plot to kill police' 16th January 2015 retrieved from http://www.bbc.co.uk/news/world-europe-30848946 [accessed 22nd January 2015]
[18] BBC News (2015) 'Greece arrests over Belgian "jihadist terror plot"' 17th January 2015 retrieved from http://www.bbc.co.uk/news/world-europe-30865316 [accessed 22nd January 2015]
[19] Kate Connelly (2015) 'Two men arrested in berlin on suspicion of recruiting for Isis in Syria' *The Guardian* 16th January 2015 retrieved from http://www.theguardian.com/world/2015/jan/16/two-men-arrested-berlin-isis-syria [accessed 22nd January 2015]
[20] BBC News (2015) 'Imran Khawaja: The jihadist who faked his own death' 20th January 2015 retrieved from http://www.bbc.co.uk/news/uk-30891145 [accessed 22nd January 2015]

terrorism police officers are currently facing as they try to prevent acts of terrorism happening and in keeping EU citizens safe. This point has been made by the Director of the EU's policing intelligence agency Europol, Rob Wainwright. He warned that the EU's policing agencies do not have the capability to monitor online communications of suspects, saying there is a security gap facing police forces in Europe who are trying to track down extremists online, with some of these extremists being effectively out of reach.[21] The potential result of this security gap is as the head of the UK's national security agency MI5, Andrew Parker pointed out when he said it is virtually impossible to prevent every type of terrorist attack.[22]

Passenger Name Record Data

The EU's Directive on Passenger Name Records 2011/0023- Information contained in Passenger Name Records Data

In February 2011 the European Commission produced a proposal for a directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[23] At the time of its publication the explanation memorandum covered issues as to why the directive was needed by agencies involved in investigating terrorism and serious crime where a comparison was drawn between PNR and aircraft passenger information (API). PNR's contain the following information:

1. Name of Passenger;
2. Contact details for the travel agent or airline office;
3. Ticketing details;
4. Itinerary of at least one segment, which must be the same for all passengers listed;
5. Name of person providing the information or making the booking;
6. Passenger gender;

---

[21] BBC News (2015a) 'Terror threat posed by thousands of EU nationals' 13th January 2015 retrieved from http://www.bbc.co.uk/news/uk-30799637 [accessed 22nd January]

[22] Security Service MI5 (2015) 'Address by the Dire-General of the Security Service, Andre Parker, to the Royal United Services Institute at Thames House 8th January 20-15' retrieved from https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-on-terrorism-technology-and-accountability.html [accessed 23rd January 2015]

[23] 2011/0023

7. Passport details (includes nationality, passport number and date of passport expiry);
8. Date and place of birth;
9. Billing information;
10. Form of payment (include debit/credit card details);
11. Contact details (potentially include landline/mobile phone numbers);
12. Frequent flyer data; and
13. Vendor remarks kept by the airline.[24]

Advanced Passenger Information data (API)

In addition to flight identification that provides the scheduled departure and arrival of flights and number of passengers on the flight, API's contains the following information in relation to each individual passenger:

1. passenger's name
2. passenger's address;
3. passenger's date of birth;
4. passenger's gender;
5. passenger's nationality;
6. passport details;
7. passenger seating;
8. visa details (where applicable).[25]

The countries that have signed up to the requirement that passengers complete API details are:

1. Antigua;
2. Australia;
3. Barbados;
4. Canada;
5. China;
6. Costa Rica;
7. Cuba;
8. Dominican Republic;
9. Grenada;
10. India;
11. Ireland;
12. Jamaica;
13. Japan;
14. Maldives;
15. Mexico;
16. Republic of Korea;
17. Russian Federation;

[24] International Civil Aviation Organisation (2010) Guidelines on Passenger Name Record (PNR) Data Quebec: International Civil Aviation organisation

[25] WCO/IATA/ICAO (2013) Guidelines on Advance Passenger Information (API) retrieved from http://www.icao.int/Search/pages/Results.aspx?k=api paragraph 8.1.5

18. Saint Lucia;
19. Spain (except for Schengen zone passengers)
20. Taiwan;
21. Trinidad & Tobago
22. Turkey;
23. United Kingdom;
24. United States

It is the responsibility of the airline to obtain the information required under API procedures.[26] Border control, customs and policing agencies in the respective states listed above can access passengers' personal data contained in the API just prior to and on the arrival of the passenger. As privacy and data protection varies from state to state the API guidelines recommendations state that the personal data:

1. Should be obtained and processed fairly and lawfully;
2. Should be stored for legitimate purposes and not be used in any way that is incompatible for these purposes;
3. Should be adequate, relevant and not excessive in relation to the purposes for which they are stored;
4. Should be preserved in a form which permits identification of the data subjects for no longer for which the data is stored.[27]

While the batch style of API systems exist between the participating states where the API is received by requesting government in advance of the flight's arrival the ability to enhance aviation security via the batch style API systems is limited.[28] This can be enhanced if the participating states adopt the interactive API system that allows a two-way communication in real time that initiated during check-in and allows for persons known or believed to pose an unacceptable risk to be identified as early as possible and persons known to be inadmissible to the state they are travelling to be identified prior to travel.[29]

Comparison between API and PNR data and the limitations of API

[26] NIDirect (2015) Advance registration before you travel retrieved from http://www.nidirect.gov.uk/advance-registration-before-you-travel [accessed 19th April 2015]
[27] WCO/IATA/ICAO 2013 paragraph 9.4
[28] Ibid paragraph 5.2
[29] Ibid paragraph 5.2

Compared to PNR data, API data is fairly limited in what information is recorded and accessed by border control and this limitation was recognised by the European Commission in the explanatory memorandum to the PNR Directive saying:

> 'API data does not enable law enforcement authorities to conduct an assessment of passengers and therefore do not facilitate the detection of hitherto "unknown" criminals or *terrorists*' [my emphasis].[30]

While API is useful in terrorism and organised crime investigations at port and border controls for investigating officers to ascertain who is on a flight list that can be checked to suspects already contained within intelligence systems, API is restrictive when trying to ascertain the identity of those who are not known on intelligence systems. Another limitation of API's compared to PNR data is while API data is available from a passenger's check-in at an airport, PNR data is transferred from 48 to 36 hours before departure from the Airline Reservation System to the Departure Control System which the border control and policing agencies can access. This gives those agencies more time to analyse the PNR data within their own intelligence systems to assess if there are any connections to terrorist or organised crime activity.[31]

However the additional information contained in the Directive such as who made the booking or contact details and methods of payment can be cross-checked to see if there is a connection with terrorist suspect in intelligence systems. As stated above, Europol have already found that groups are facilitating the travel of individuals who may referred to in intelligence circles as clean-skins, that is they are not on any intelligence system. However if from the PNR data a link is made, this will greatly assist the officer in agencies investigating

[30] 2011/0023 Directive p.7

[31] ICAO/WCO/IATA (2015) Management Summary on Passenger-related Information [Umbrella Document] retrieved from http://www.icao.int/Search/pages/Results.aspx?k=api [accessed 17th April 2015] p.2

terrorism. The fact that PNR data is an important intelligence tool is also recognised in the PNR Directive's explanatory memorandum.[32]

Key Provisions in the 2011 PNR Directive

While clearly stating the scope of use of PNR data was the prevention, detection and prevention of terrorist offences and serious crime[33] the Directive recommended that Member States identified competent authorities to process the PNR data issued form Passenger Information Units.[34] It is clear that no decision should be taken by the competent authority on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life. One concern with the Directive related to data retention was the protection of personal data and the transfer of data to third countries. In essence, the proposed period of detention of data by competent authority was 30 days, with the Passenger Information Unit to retain the data for 5 years.[35] The protection of the data should be covered by the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[36] The data subject has the right to expect the competent authority to fulfil their duties regarding their duties under the Framework Decision (article 18) and that includes the right for the data subject to have a judicial remedy for any breach of the rights guaranteed to them by the applicable national law.[37]

PNR data sharing between the EU and Third Countries

Where the PNR data is transferred to a third country the Framework Decision makes it clear that it has to be ensured that the third country had an adequate level of protection of

[32] Directive 2011/0023 Explanatory Memorandum p.8
[33] Directive 2011/0023 article 9
[34] Directive 2011/0023, article 5
[35] Directive 2011/0023 article 9
[36] FD 2008/977/JHA
[37] FD 2008/997/JHA article 20

the intended data processing.[38] Agreements in the exchange of data currently exist. For example between the European Union and the United States there is an agreement regarding the transfer of PNR data[39] and between the EU and Australia.[40]

In the agreement between the US and the EU it states the US will confirm that effective administrative, civil and criminal enforcement measures are available under US law for privacy incidents and the US Department of Homeland Security will take disciplinary action against persons responsible for inappropriate use of the privacy conditions.[41] It also says in the agreement that the Department of Homeland Security will inform the relevant EU authorities of cases of privacy incidents involving PNR of EU citizens.[42] Similar provisions relating to data security and integrity also are present in the agreement between the EU and Australia[43]including the separate storing of EU citizens' PNR data and it is only stored for the purpose of matching with intelligence data Australian authorities have on persons suspected of being involved in terrorism or serious crime.[44] The EU has understandably taken a strict approach as to how intelligence and citizens' personal data is handled and dealt with by state authorities as provided in the European Commission's overview of information management (Communication from the Commission to the European Parliament and Council: Overview of information management in the area of freedom, security and justice COM(2010)385 final) which concludes saying:

[38] FD 2008/997/JHA article 14
[39] Agreement between the United States of America and the European Union on the use and transfer of Passenger Name records to the United States Department of Homeland Security 17434/11
[40] Agreement between the European Union and Australia on the processing and transfer of Passenger name records (PNR) data by air carriers to the Australian Customs and Border Protection Service 10093/11
[41] 17434/11 article 5(6)
[42] 17434/11 article 5(4)
[43] 10093/11 article 9
[44] 10093/11 article 9(1)(a)

> 'Adopting … a principled approach to policy development and evaluation is expected to enhance the coherence and effectiveness of current and future instruments in a manner that fully respects fundamental rights.'[45]

This is seen in the current Directive regarding the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences[46] that is expected to be introduced in 2016.

Wider Surveillance on Electronic Communication

In March 2015 the UK's Intelligence and Security Committee of Parliament (ISC) published is report on privacy and security where among its key findings it states the legal framework in the UK on surveillance, especially in relation to electronic communications has developed piecemeal and is unnecessarily complicated resulting in the Committee having serious concerns in the, '…resulting lack of transparency, which is not in the public interest.'[47] As a result among its recommendations is the key recommendation that all the current legal frameworks on surveillance are replaced a new Act of Parliament governing the intelligence and security agencies consolidating the legal current provisions.[48] The ISC added in their recommendations that new legislation should clearly list the intrusive capability that specifies:

1. The purposes for which the intrusive power is used including the protection of national security or the detection or prevention of serious crime;
2. The overreaching human rights obligations constraining such use;
3. Whether the capability is to be used in the pursuit of a specific person, location or target or in relation to a wider search to discover unknown threats;

[45] Communication from the Commission to the European Parliament and Council: Overview of information management in the area of freedom, security and justice COM(2010)385 final p.28
[46] Directive of the European Parliament and of the Council on the protection of individuals data 2012/0010 (COD)
[47] Intelligence and Security Committee of Parliament (2015) 'Privacy and Security: A modern and transparent legal framework' London: Her Majesty's Stationary Office, p/2
[48] Ibid p. 118

4. Authorisation procedures must include review, inspection and oversight, that should be carried out by the judiciary;
5. Retention periods, methods of storage and destruction arrangements;
6. The circumstances (including the constraints) in which any intelligence obtained may be shared with intelligence, law enforcement or other bodies in the UK or overseas partners;
7. Transparency and reporting requirements.[49]

The ISC also examined authorisation for carrying out electronic surveillance that included a summary of the expected collateral intrusion, including an estimate of the numbers of innocent people who may be impacted and the extent to which the privacy of those innocent people will be intrude upon.[50]

The ISC's findings have not been universally welcomed. The UK civil liberties group, Liberty in their report to the ISC during the ISC's inquiry into privacy and security the group says they have no confidence in the ISC's ability to, '…provide effective oversight of the security agencies'.[51] Underpinning this view is Liberty's perception that the ISC is inadequately staffed and funding and in not having sufficient expertise. However its more scathing criticism of the ISC is Liberty's assertion that the ISC's annual reports:

> 'consistently fail to critically analyse the agencies' claims and its recommendations to not seek to hold the agencies' to account but rather "do the agencies" bidding on matters as varied as funding and the creation of closed courts. …Liberty regards the ISC more as a spokesperson of the agencies than a credible oversight body.'[52]

This view of the ISC came out when members of four privacy campaign groups gave evidence to the ISC's inquiry into privacy and security where in essence they objected to the principle of collecting internet communications in bulk. When members of the Committee asked the four privacy campaigners if evidence emerged through bulk data collection that led

[49] Ibid pp.118-119
[50] Ibid p.119
[51] Liberty (2014) 'Liberty's evidence to the Intelligence and Security Committee's inquiry into Privacy and Security' retrieved from http://www.liberty-human-rights.org.uk/policy/ [accessed 20th March 2015] p.4
[52] Ibid, p.4 paragraph 5

to terrorists being arrested and terrorist attacks being prevented and rather than allow intelligence agencies to use bulk data collection methods, as a matter of principle they believe so strongly that bulk data collection is unacceptable that terrorist attacks is a price a free society has to pay. The four privacy campaigners said it was with Isabella Sankey, the director of policy at the group Liberty said, 'Yes …That is the price you pay to live in a free society.'[53] When asked by the Committee if her view would change if the electronic bulk data collection was authorised under a legal framework, Sankey's reply was, 'No'.[54]

For some reading this Liberty's response may appear astounding and irresponsible and for others this stance is plausible. What this shows is how polarised views are on practises related to surveillance of electronic communications that gathers bulk data collection. Where such an extremist position is taken in relation to the protection of an individual's liberty and data protection as that by Liberty it does not assist in reaching realistic compromises in both the law or in governmental policy directing agencies involved in surveillance. The interests of national security and individual liberty are not exclusive, they are inclusive. They are not opposing poles but a seamless web of protection incumbent upon the state.[55]

Concerns over the Surveillance Society: The Snowden Revelations

In April 2013, the Committee on Civil Liberties of the European Parliament (LIBE) saw the PNR Directive being too wide and consequently refused to agree for the need of the Directive. The concerns mainly cantered on Passenger Information Unit as having the potential to refuse to erase a person's data even if they are not suspected of a crime and the Committee had a concern the Directive left it open to authorities to carry out offender

[53] Intelligence and Security Committee of Parliament (see note 47) pp. 35-36
[54] Ibid p.36
[55] International Commission of Jurists, (2009) Assessing Damage, Urging Action Geneva: ICR, p.21

profiling on individuals who matched certain behaviour.[56] 2013 was a year where fears of a surveillance society were confirmed following the revelations by the former US National Security Agency (NSA) employee, Edward Snowdon on the practices of the NSA and the UK's General Communications Headquarters (GCHQ) in particular Operation PRISM and the bulk surveillance of electronic forms of communication and telephone use, some of which was unauthorised.[57] The shock waves of the NSA's actions reverberated around the world, more so when it was revealed that politicians in the EU's Member States were also spied on by the NSA, in particular the German Chancellor Angela Merkel.[58] As Greenwald (the *Guardian* newspaper journalist Snowden passed the NSA documentation onto) says, what is more remarkable are the revelations that the NSA was spying on millions of European Citizen adding;

> '…in addition to foreign leaders the United states … also spied extensively on international organisations such as the United Nations to gain a diplomatic advantage.'[59]

It is understandable why there is such a concern in recommending further powers of surveillance to national security and policing agencies, yet a balance has to be drawn between the needs of protecting the interests of security within the EU's Member States and the rights of individual citizens.

In June 2013 the UK newspaper *The Guardian* and the US newspaper *The Washington Post* broke with the news story regarding the NSA and the Prism programme that gave US Federal agencies direct access to servers in the biggest web firms including Google,

---

[56] The European Citizen (2014) 'Draft EU PNR Directive voted down at Committee Stage' retrieved from http://theeuropeancitizen.blogspot.co.uk/2013/04/draft-eu-pnr-directive-voted-down-at.html [accessed 7th September 2014]

[57] Greenwald, Glenn (2014) No Place to Hide: Edward Snowden, the NSA and the US Surveillance State New York: Metropolitan Books, pp.33-42

[58] Ibid p.141

[59] Ibid p.142

Microsoft, Facebook, Yahoo, Skype and Apple.[60] Snowdon released top secret documents to a *Guardian* journalist, Glenn Greenwald who, in the first of a number of reports, revealed the NSA was collecting telephone records of millions of US customers under a top secret order issued in April 2013 adding that, '…the communication records of millions of US citizens are being collected indiscriminately and in bulk regardless of whether they are suspected of any wrongdoing'.[61] Adding the NSA's mission had transformed from being exclusively devoted to foreign intelligence gathering Greenwald said it now focused on domestic communications.

As the revelations from the documents Snowdon passed on regarding the FSA's activities increased, *The Guardian* reported that GCHQ also gained access to the network of cables carrying the world's phone calls and Internet traffic and processed vast streams of sensitive personal information, sharing this with the NSA.[62] This followed on from earlier reports that GCHQ accessed the FSA's Prism programme to secretly gather intelligence, where between May 2012 –April 2013, 197 Prism intelligence reports were passed onto the UK's security agencies, MI5, MI6 and Special Branch's Counter-Terrorism Unit.[63] GCHQ's actions led to the German Justice Minister writing to British ministers regarding an allegation of mass surveillance by British intelligence asking for reassurance the actions were legal and if they were targeting German citizens.[64] With reports from *The Guardian* that FSA actions were posing a threat to the privacy of EU citizens, this was a cause of concern for the EU's

[60] BBC News 7th June 2013 'Web Privacy – outsourced to the US and China? Retrieved from http://www.bbc.co.uk/news/technology-22811002 [accessed 1st September 2013]
[61] Greenwald, G. (2013) NSA collecting phone records of millions of Verizon customers daily *The Guardian* 6th June 2013 retrieved from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [accessed 1st September 2013]
[62] MacAskell, E, Borger, J., Davies, N. and Ball, J. (2013) GCHQ taps fibre-optic cables for secret access to world's communications *The Guardian* 21st June 2013 retrieved from http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [accessed 1st September 2013]
[63] Hopkins, N. (2013) UK gathering secret intelligence via covert NSA operation *The Guardian* 7th June 2013 retrieved from http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism [accessed 1st September 2013]
[64] BBC News 25rth June 2013 'Germany seeks UK surveillance assurance' retrieved from http://www.bbc.co.uk/news/uk-23048259 [accessed 1st September 2013]

Justice and Home Affairs (JHA) resulting in EU's Justice Commissioner Viviane Reding stating:

> 'The European Commission is concerned about the possible consequences on EU citizens' privacy. The Commission has raised this systematically in its dialogue with the US authorities, especially in the context of the negotiations of the EU-US data protection agreement in the field of police and judicial co-operation…'[65]

During this dialogue the difference in legal culture between the EU and the US raised its head regarding individual's rights in the respective jurisdictions with the EU's focus being the dignity of citizens. In protecting fundamental human rights under the aegis of the rule of law the EU requires a system of protection of an individual citizen's data privacy.[66] There is no such explicit protection to a general right to privacy under the US Bill of Rights rather it is inferred in the First, Fourth, Fifth and Ninth Amendments.[67] This is important as Snowdon's revelations had the potential to damage not only diplomatic relations between the US and EU Member States, but also affect the terrorism intelligence sharing between European counter-terrorism agencies via Europol and US federal agencies. To prevent US/UK diplomatic relations with the rest of the EU Member States deteriorating further, senior US and UK politicians were forced to speak openly and defend the actions of the FSA and GCHQ. The UK's Foreign minister, William Hague said that both nations, '…operated under the rule of law', with GCHQ being, '…scrupulous in complying with the law' and used the intelligence to protect citizens' freedoms.[68]

---

[65] Watt, N (2013) Prism scandal: European commission to seek privacy guarantees from US *The Guardian* 10th June 2013 retrieved from http://www.theguardian.com/world/2013/jun/10/prism-european-commissions-privacy-guarantees [accessed 1st September 2013]

[66] Murphy, C.C. (2012) EU Counter-Terrorism Law: Pre-Emption and the Rule of Law Oxford: Hart Publishing, p.149

[67] Whitman, J.Q. (2004) The Two Western Cultures of Privacy: Dignity versus Liberty 113 *Yale Law Journal* 1151—1221, p.1155

[68] BBC News 26th June 'US-UK intelligence-sharing indispensable says Hague' retrieved form http://www.bbc.co.uk/news/uk-politics-23053691 [accessed 2nd September 2013]

As a result of handing the secret documents to journalists the US Justice Department filing criminal charges against Snowden for espionage and theft of government documents and a provisional arrest warrant was issued by a federal court in the Eastern District of Virginia.[69] To evade prosecution Snowden left the USA where he was granted temporary asylum by the Russian Government, causing further friction in the political relations between the US and Russia.[70] Referring to 'top secret' documents Snowden passed on to them, *The Guardian* reported that from 2010-2013 the US government paid GCHQ £100 million to secure access and influence over the UK's intelligence gathering programmes.[71] As these revelations were claiming to come from the secret documents Snowden passed on to Greenwald, it triggered the security services to act to retrieve the documentation at the earliest opportunity.

It is not Just a UK Issue: Digital Rights Case and EU Directive 2006/24/EC on Data Retention

Of the recent decisions by the European Court of Justice (ECJ) on data retention and privacy protection is that of the Grand Chamber in *Digital Rights Ireland Ltd v Minister for Communications and others*.[72] The case centred mainly on Directive 2006/24/EC that lays down the obligation on the providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed by them. The ECJ also considered the provisions of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy with the aim to harmonise Member States' legal provisions regarding the protection of fundamental rights and freedoms especially in the processing of personal data in the electronic sector. In essence the ECJ found

[69] BBC News 22nd June 2013 'NSA leaks: US charges Edward Snowden with spying' retrieved from http://www.bbc.co.uk/news/world-us-canada-23012317 [accessed 1st September 2013]
[70] BBC News 1st August 2013 'NSA spy leaks: Snowden thanks Russia for asylum' retrieved from http://www.bbc.co.uk/news/world-europe-23541425 [accessed 2nd September 2013]
[71] Hopkins, N. and Borger, J. (2013) Exclusive: NSA p[pays £100m in secret funding for GCHQ The Guardian 1st August2013 retrieved from http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [accessed 2nd September 2013]
[72] Joined Cases C-293/12 (Digital Rights) and C-594/12 (Karntner Landesregierung)

that the 2006 and the 2002 Directives were inlaid in relation to the retention of data processed in connection with the provision of available electronic communications data. Key to this decision was article 4 of the 2006 Directive that states member States shall adopt measures to ensure that data retained is provided only to the competent national authorities in specific cases in accordance with national law adding:

> 'The procedures to be followed and the conditions to be fulfilled ion order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member state in its national law, subject to the relevant provisions of EU law or public international law and in particular the [European Convention on Human Rights] as interpreted by the European Court of Human Rights'[73]

The ECJ said that EU legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against unlawful access and use of that data.[74]

Looking at the inadequacies of article 4 in the 2006 Directive the ECJ held that article 4 did not expressly provide that access to the use of the data was strictly restricted for the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such crimes; all the conditions specified in article 4 as that Member States defined procedures to followed that were in accordance with necessity and proportionality requirements.[75] Examining the provisions of article 7 of the 2006 Directive regarding data protection and security that the ECJ said should be read in conjunction with article 4 held that it does not ensure a particularly high level of protection and security and the Directive as a whole did not ensure the irreversible destruction of the data at the end of

[73] Article 4 EU Directive 2006/24
[74] *Digital Rights* Case C-293/12, paragraph 54
[75] D*igital Rights* Case C-293/12, paragraph 61

the data retention period.[76] The ECJ did recognise the importance of data retention in relation to investigations into serious crime and terrorism saying:

> '…it is of the upmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques'[77]

In saying this, the ECJ held that it was the fact the 2006 Directive's data retention measures were too vague to even justify these objectives as the rationale for the data retention. Simply stating retention should be carried out under the principles of necessity and be proportionality cannot be justified in imposing limitations on citizens' rights as the imposition of limitations requires a legitimate aim and terrorism is certainly a legitimate aim that is recognised as one that meets the objective s of general interest recognised by the EU and that includes corresponding with the need to protect the rights and freedoms of others, including the important right, the right to life. As Ojanen in his analysis of the Digital Rights Case states, the moor systemic and wide the collection, retention and analysis of bulk data becomes, the closer it can be seen as moving towards the core area of privacy and data retention adding:

> '…the closer it can be seen as moving towards the core area of privacy and data protection with the outcome that at least the most massive, systematic forms of collection and analysis of [bulk data] can be regarded as constituting an intrusion into the inviolable core of privacy and data protection'[78]

As Ojanen recognised, the ECJ decision in Digital Rights is not a 'total knockout' to mandatory retention[79] what is needed is by the EU in drawing up legislation is that specifically gives the legitimate aim for the retention being to support investigations into acts of terrorism or serious organised crime such as human trafficking, specifying realistic periods

[76] *Digital Rights* Case C-293/12, paragraph 67
[77] *Digital Rights* Case C-298/12, paragraph 51
[78] Tuomas Ojanen (2014) 'Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance' *European Constitutional Law Review* 10(3), 528-541, at p. 537
[79] Ibid, p. 539

of data retention and sufficient safeguards into protecting rights of privacy and data protection.

EU Data Protection and Privacy Laws

European Union law is clear that personal data is to be protected. Article 16 of the Treaty on the Functioning of the European Union (TFEU) states that everyone has the right to the protection of personal data concerning them[80] and the European Parliament and the Council must act in accordance with ordinary legislative procedure that will lay down rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, office and agencies when carrying out activities that fall with the scope of EU law[81] as does article 39 in the Treaty of Union. The Charter of Fundamental Rights of the European Union also is clear that everyone has the right to the protection of personal data concerning them.[82] In that right it states, '…data must be processed fairly for specified purposes on the basis of consent of the person concerned *or some other legitimate basis laid down by law'* [83] [My emphasis]. This is in addition to the respect the state must have for the right of a person to their private and family life in both the Charter of Fundamental Rights of the European Union[84] and the Council of Europe's European Convention of Human Rights (ECHR) (Article 8). Article 8 of the ECHR does allow for the state to interfere with the right to privacy where it is under an act proscribed by law and it is necessary in democratic state when it is in the interests of national security or to prevent crime or disorder.

New EU Data Protection Regulation and Directive

The EU was looking to amend the data protection provisions it currently has in place prior to the Snowden revelations, however the EU is introducing changes to take effect by

[80] TFEU C326/55 Article 16(1
[81] TFEU article 16(2)
[82] 2000/C 364/01 Article 8(1)) 8(2)
[83] 2000/C 364/01 Article 8(2)
[84] 2000/C 364/01 Article 7

2016 at the latest that will tighten up EU citizens' data protection, in particular regarding data exchange with third countries. The two pieces of legislation proposed are:

- Personal data protection regulation: processing and free movement of data (General Data Protection Regulation);[85]
- Personal data protection directive: processing of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties and free movement of data.[86]

The regulation will have an impact in the private sector as businesses will have to set up new processes to facilitate the rights of citizens to access information held on them. Regarding the directive, the transfer of data to a third country/international organisation will only occur if it is for the same purpose as the directive and that organisation is a public authority in a state that provides a proper level of data protection within a country where appropriate safeguards are established in a legally binding instrument (article 33).

Post the January 2015 terrorism events in Europe, the EU's Justice and Home Affairs Commission has brought back on the EU's legislative agenda a proposal for blanket collection and storage of passenger name record data for up to five years on all records of passengers flying in and out of Europe. It is not a given that the plans will become legislation in the EU as the vice-chairman of the European Parliament's civil liberties committee, Jan Philip Albrecht sees the plans as an affront, in particular to the EU's main court, the European Court of Justice decision in *Google Spain SL, Google Inc. v Agencia Espanola de Prrteccion de Datos (APED)*[87], which held in 2014 that data retention without any link to risk

[85] 2012/0011 COD
[86] 2012/0010 COD
[87] Case C-131/12

or suspicion is not proportionate. For Albrecht a plan to blanketly retain all passenger data would be open to a breach of fundamental rights.[88]

Surveillance of Electronic Communication and Bulk Data Directive

Internet an Communications Service Providers Lack of Disclosure in Suspected Terrorism Related Communication

In the UK's Intelligence and Security Committee of Parliament (ISC) report on the intelligence relating the murder of Fusilier Lee Rigby by Michael Adebolajo and Michael Adebowale outside Woolwich Barracks, London in May 2013 concern was expressed in the report that Adebolajo and Adebowale's electronic communication with known sources of information including those from Al Qaeda in the Arabian Peninsula (AQAP) based in Yemen was not picked up by the UK's national security or counter-terrorism policing officers.[89] One piece of communication that was not acted on was communication via Facebook between Adebowale and AQAP operative referred to as FOXTROT, who was not known at the time to UK national security or counter-terrorism policing agencies, in late 2012. In the communications with FOXTROT Adebowale expressed in a graphic and emotive manner his desire to murder a British soldier. FOCTROT encouraged Adebowale and suggested several methods of how he could successfully carry out the attack.

The company on whose system the online exchange took place between Adebowale and FOPXTROT closed some of Adebowale's accounts before the murder of Lee Rigby was carried out. In their inquiry leading to the report the ISC learnt that internet and communications service providers use various automated techniques for

[88] Travis, Alan (2015) 'European counter-terror plan involves blanket collection of passengers' data' The Guardian 28th January 2015 retrieved from http://www.theguardian.com/uk-news/2015/jan/28/european-commission-blanket-collection-passenger-data [accessed 28th January 2015]

[89] Intelligence and Security Committee of Parliament (2014) 'Report on the intelligence relating tot eh murder of Fusilier Lee Rigby' London: HMSO, pp.119-136

identifying accounts they provider believes are breaking the terms of service such as those linked to child exploitation and to illegal acts such as inciting violence.[90] One might expect that the ISP and CSP companies would routinely pass information relating to communications of this type to the relevant authorities, but as GCHQ reported to the ISC the authorities only instigate actions when they receive a tip off or a complaint from another user or an authority. GCHQ added that for accounts linked to terrorism, information is rarely passed to the authorities unlike child exploitation cases where ISP and CSP's *regularly* pass on information to the appropriate authorities.[91]

Even though it was clear that Adebowale's eleven social media accounts were linked to terrorist activity the company disabled the accounts as a result of an automated process and did not manually review the content of the accounts nor pass on any information to the relevant authorities. Regarding this practice by ISP and CSP's, the tone of the ISC's report recommends that even if the ISP or CSP does not take action themselves to interrogate an account with suspected links to terrorism they could notify the relevant authorities that they had detected such an account adding:

> 'In the case of Adebowale, has MI5 been told that there was further intelligence to suggest that he was in contact with terrorist organisations, this might have led to different investigative decisions, which might in turn have led them to Adebowale's exchange with FOXTROT in December 2012'.[92]

As a result the ISC recommended that when possible links to terrorism trigger accounts to be closed the ISP and CSP's accept their responsibility to review the accounts immediately and if the review provides information of a specific intention to commit a terrorist act is present to pass this information onto the appropriate authority. It is such a policy adopted by ISP and CSP's that has led to the Director of GCHQ saying:

---

[90] Ibid p.128
[91] Ibid p.128
[92] Ibid p.129

> ‘However much [technology companies] may dislike it, they have become the command-and-control networks of choice for terrorists and criminals’.[93]

This situation is not unique to the UK, this is an international problem and requires an international response for which the EU is well placed to take a lead on. If this is not done then Member States will take unilateral decisions or though bi-lateral agreements with other nation states action to take a legislative position regarding the requirement that ISP and CSP’s co-operate to supply of information that is suspected to be terrorist related. A problem with such a scenario is that many ISP and CSP’s are based outside many Member States, even the EU itself and as such are not obliged to retain and provide communications data to relevant authorities. However the EU represents 28 states and as such it has the potential leverage to encourage third countries such as the US, Canada, and those states with whom the EU and EU Neighbourhood Polices agreement. *Prima facie* this may appear an idealistic and naive suggestion, but international pressure, demonstrating the concerns for national security an issue underpinned by the right to life of citizens, where negotiations with ISP and CSP’s occur to draw up a uniform policy in forwarding of communications data to relevant authorities is more likely to obtain co-operation with ISDP and CSP’s. One reason why the EU is ideally placed to take the lead is that rights to privacy and data protection are embedded in EU law. It is the protection of their customers’ privacy that is sacrosanct with ISP and CSP’s. The position the EU holds in relation to privacy and data protection makes the EU more likely to be heard by ISP and CSP’s as an approach that is simply one of compulsory supply of data without clear and enshrined data protection is not the ideal approach to take with companies, especially here you are looking for co-operation. As such this will help to ensure the needs of national security are balanced with the rights to privacy and data protection is equitably balanced.

93

The Example of the UK's Response to the Digital Rights Case

In response to the ECJ's decision in the *Digital Rights* case and in order to replace the 2006 Data Retention Directive[94] an example of a Member State taking a unilateral response to this issue is the UK and the Data Retention and Investigatory Powers Act 2014 (DRIPA). Section 1 DRIPA allows the Secretary of State to issue a notice to ISP and CSP's to retain relevant communications data (a retention notice) if the Secretary of State considers the requirement to be necessary and proportionate where:

1. It is in the interests of national security;
2. To prevent or detect crime or preventing disorder;
3. It is in the interests of the UK's economic well-being; it is in the interests of public safety;
4. It is for the purposes of protecting public health;
5. It is for the purpose if assessing or collecting tax, duty or levy or other imposition, contribution or charge payable to a government department;
6. It is for the purpose in an emergency of preventing death or injury or any damage to a person's physical or mental health or of mitigating any injury or damaged to a person's physical or mental health;
7. It is for a purpose which is specified by the Secretary of State.[95]

In doing so the retention notice can relate to a particular operator or any description of operators where the notice will require the retention of all data or of the type described in the notice and specify the period the data should be detained,[96] with the maximum period of data retention not exceeding 12 months.[97] In order to make requests on ISP and CSP's on a lawful footing DRIPA has amended section 5 (3) of the Regulation of Investigatory Powers Act 2000 (RIPA) that is concerned with the grounds necessary for issuing of warrants to intercept communications, adding the issuing of a warrant is

[94] Data Retention and Investigatory Powers Act 2014 Explanatory notes, paragraph 3
[95] S.1(1) Data Retention and investigatory Powers Act 204 and section 22(2) Regulation of Investigatory Powers Act 2000
[96] S.1(2) Data Retention and Investigatory Powers Act 2014
[97] S1(5) Data retention and Investigatory Powers Act 2014

necessary where in the circumstances it appears to the Secretary of State the warrant is relevant to the interests of national security.[98]

Where a nation state legislates the granting of powers for the likes of retention notices and warrants is all well and good when applying to companies located within that state but the law of one state is not normally applicable to companies located outside that state, and many ISP and CSP's are located outside the UK, which can in effect make these powers redundant. DRIPA has tried to address this issue by amending RIPA to allow for an interception warrant to be delivered at the company's principal office within the UK and if that company does not have a principal office at any place in the UK here that company carries on their business or conducts its activities.[99] Should there still is non-compliance by that company is outside the UK to the warrant DRIPA amends section 11 of RIPA to give effect that the warrant is enforceable by civil proceedings.[100] To assist in ensuring there are ways of improving the access of electronic communications data the UK appointed its former US Ambassador, Sir Nigel Sheinwald as a special envoy on intelligence and law enforcement data sharing. His role is lead discussions with key international partners and ISP and CSP's seeking to:

1. Identify ways of taking forward the UK Government's relationships with ISP and CSP's to ensure the UK Government's work is coherent with its broader relationship with these providers;
2. Consider wider international arrangements in this area;
3. Ensure that any new arrangements observe the requirement that data is requested and provided only where necessary and proportionate for the purposes of national security and the prevention or detection of serious crime;
4. Other measure to work with the US on the range of options to strengthen reliable access through Mutual legal Assistance Treaty systems, other legal or

[98] S.3(2) Data Retention and Investigatory Powers Act 2014
[99] S4(2) Data Retention and Investigatory Powers Act 2014
[100] S.4(5) Data Retention and Investigatory Powers Act 2014

> political frameworks or remedies for better arrangements for direct requests form UK agencies to companies that hold the data.[101]

It is submitted that in essence one nation state like the UK that attempts to apply a tough legal stance against large transnational companies such as Facebook, Twitter and other ISP and CSP's will not encourage compliance by these companies to request and can only result in protracted legal battles that could in effect cost the state more both financially as well as politically. This example demonstrates why it is preferable for nation states to work together when making requests with ISP and CSP's in relation to data retention and in gaining access to certain information, even when related to acts of terrorism. As stated, due to the emphasis it places on rights to privacy and data protection the EU is not only best placed to take a lead but ethically it is best positioned to negotiate alongside third countries with ISP and CSP's to assist in the fight against terrorist by simply manually reading communication where it is suspected that communication is related to terrorism.

The Category of Data Subject of Wider Surveillance

This proposal is not advocating for a blanket interception of electronic communication, this proposal is requesting that consideration be given to introducing legislation that allows for wider powers of surveillance of targeted electronic communication related to terrorism. Communications data includes details of time, duration, originator and recipient of communication that is the who, when and where of communication, but not the content of the communication itself.[102] Breaking it down to three distinct categories communications data include:

---

[101] UK Government Press release (2014) Sir Nigel Sheinwald appointed Special Envoy on intelligence and law enforcement data sharing retrieved from https://www.gov.uk/government/news/sir-nigel-sheinwald-appointed-special-envoy-on-intelligence-and-law-enforcement-data-sharing [accessed 21st May 2015]

[102] Simon McKay (2015) 'Covert Policing: Law and Practice' (2nd edition) Oxford: Oxford university Press, p.129

1. Traffic Data – is where communications is or may be transmitted through a telecommunications system that identifies a person, the apparatus used or the location to and from the communication is made. It can identify or select the apparatus by which the communication is transmitted. Traffic data comprises of signals for the actuation of the apparatus used for the purposes of a telecommunications system for effecting the transmission of the communication. It also can identify the time at which the communication occurs or can identify the data comprised in or associated with the communication;
2. Use Data – relates to the actual information related to the use made by the person of a telecommunications service or is in connection with the provision or sue by a person of a telecommunications system, but does not contain the contents of any communication. In other words it is simply the data relating to the use made by a person of a communications service;
3. Subscriber Data – this is the information held or obtained by the ISP or CSP where the information is about the person using the service provided by the ISP or CSP. This will include information on people who are subscribers to an ISP or CSP without necessarily using that service and those who use communications without necessarily subscribing to it[103]

This is bulk data (also referred to as metadata) and while not being able to see the content of communications it allows national security and counter-terrorism agencies to trace and acquire information on the movements of a person. It is essential that in allow such agencies to carry out surveillance on electronic communications data that there are stringent controls in place in both the granting of an authority to carry out this type of surveillance.

Europol and Intelligence Exchange

Legislative Changes making Europol an EU Body

One issue that could cause a blockage to these proposals is the current position of Europol, especially in relation to working with Member States' national security agencies. Two important documents have raised the importance of the role Europol plays in assisting in counter-terrorism and crime investigations, the EU Council Decision of the 6th April 2009 establishing Europol[104] and articles 87 and 88 of the

[103] Ibid, pp.129-130, UK Draft Communications Data Bill 2012 p.7, Home Office (2014) 'Retention of Communications Data: Code of Practice' London: HMSO, paragraph 2.7
[104] Council Decision 6th April 2009 establishing the European Police Office (Europol) (2009/371/JHA)

Lisbon Treaty. The 2009 Council Decision has in effect transformed Europol into a European agency as evidenced by its funding by the EU budget, the formalising of Europol's staffing structure and changes regarding Europol's co-operation with third countries and organisation.[105] The 2009 Council Decision gives Europol a legal personality[106] where it states Europol's objective is to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in combating terrorism (and organised crime and other forms of serious crime).[107] Article 88(1) of the Lisbon Treaty states Europol's mission:

> '…shall be to support and strengthen action my Member States' police authorities and other law enforcement services and their mutual co-operation in preventing and combating serious crime affecting two or more Member States, *terrorism* and forms of rime which affect a common interest covered by a Union policy.' [my emphasis]

There are two problems that still exist in relation to Member States' attitudes towards sharing intelligence with Europol. They are the ability for Member states to negotiate their own bi-lateral or multi-lateral agreements and it appears that there is no obligation on Member States' national security agencies to co-operate with Europol.

Bi-Lateral Agreements Undermining Europol

Coolsaet observes that involvement of more actors in the counter-terrorism endeavour at Europol has, '…reignited the traditional reluctance of member States to transfer confidential information to the organisation'.[108] Added to this, what is hindering Europol's effective functioning as Europe's primary law enforcement agency is Member States' national preference for bilateral relationships and the parallel

[105] Christian Kaunert and Sarah Leonard (2011) EU Counterterrorism and the European Neighbourhood Policy: An Appraisal of the Southern Dimension *Terrorism and Political Violence* 23(2) 286-309, p.294
[106] [n 112] article 2(1)
[107] [n 112] article 3
[108] Rik Coolsaet (2010) 'EU counterterrorism strategy: value added or chimera?' *International Affairs* 86(4) 857-873, p.864

participation in informal, practitioner-led networks.[109] The effect of this is in limiting the capability of Europol's co-operation, and that is not just between EU Member States but with Europol's co-operation agreements with third countries. As Kaunert and Leonard point out, while Europol has described its co-operation with the US counter-terrorism agencies as excellent;

> '…[Europol] has acknowledged that its cooperation with the FBI has been more limited so far, because the FBI has been encouraged to prioritise its bilateral liaison network of legal attachés in the embassies of EU Member States'[110]

The establishment of bi-lateral agreements and the lack of full co-operation between EU Member States and Europol can be traced over the last decade, even up to the present day. Examples of these close international relations on terrorism related issues include the UK with Pakistan and France with Algeria as well as Germany allowing US prosecutors and FBI agents to carry out investigations with a German federal prosecutor.[111] Perhaps the prime example of how up to 2010 EU Member States undermined Europol is through the signing of multi-lateral agreements outside the EU. The best two examples are seen with the 2003 G6 Agreement and the 2005 Prum Treaty. The G6 was established in May 2003 and consists of the six largest EU Member States (UK, France, Germany, Italy, Spain and Poland, who joined in 2006) who out of frustration with the EU's bureaucratic JHA structures set up the G6 group to discuss issues of internal security, including terrorism.[112] The G6 was not simply a talking shop. In 2005 it agreed to create a common database of individuals suspected of connections to terrorist organisations and in March 2006 it agreed to create multilateral police

[109] Ibid p.864
[110] [n113] p.293
[111] Keohane, D. (2008) The Absent Friend: EU Foreign Policy and Counter-Terrorism Journal of Common Market Studies 46(1), 125-146, p.128-129
[112] Bures, O. (2008) Europol's Fledgling Counterterrorism Role Terrorism and Political Violence 20(4), 498-517, p.506, Javier Argomaniz (2012) The EU and Counter-Terrorism: Politics, polity and polices after 9/11 London: Routledge, pp.51-52

support teams in cases of serious terrorist attacks, as well as joint investigation teams to investigate terrorism and organised crime.[113] In May 2005 seven EU Member States, the Netherlands, Belgium. Luxembourg, Austria, France, Germany and Spain signed the Prum Treaty to step up cross-border co-operation, particularly in combating terrorism and the Treaty includes an exchange system of DNA profiles, fingerprints, vehicle registration data and data on aircraft security.[114] As a result Europol's work has been seen as merely complementing a Member State's national agency's own analysis and the multi-lateral co-operation established with other services.[115]

However there have been positives in Europol developing agreements with third countries in the European Neighbourhood Policy (EPN) as seen in the Middle East and the Maghreb resulting in agreements between Europol and Morocco, Jordan, Algeria[116] and Israel that has built up strong co-operation in the area counter-terrorism.[117] Even with these Southern Mediterranean ENP's there are obstacles to developing co-operation on terrorism issues. There are two key reasons for this. One reason being Western states involvement in conflicts in Middle East and North African conflicts which included EU member States such as Iraq in 2003. Secondly, many of the Southern Mediterranean ENP states are not democratically elected governments and those with authoritarian tendencies are more likely to try and enhance their popularity by not complying with Western requests for co-operation.[118] In relation to international terrorism, while the EU has some responsibilities for strategic decision making, it does not play a significant operational or practical role in the

[113] Den Boar, M, Hillebrand, C and Nolke, A (2008) Legitimacy under Pressure: The European Web of Counterterrorism Networks Journal of Common Market Studies 46(1), 101-124, p.117
[114] [n120] Bures pp. 506-507, Argomaniz p.52
[115] Muller-Wille, B. (2008) The Effect of International Terrorism on EU Intelligence Co-operation Journal of Common Market Studies 46(1), 49-73, p.58
[116] Joffe , G. (2008) The European Union, Democracy and Counter-terrorism in the Maghreb Journal of Common Market Studies 46(1), 147-171, p.164, Kaunert, C. (2010) Europol and EU Counterterrorism: international Security Actorness in the External Dimension Studies in Conflict & Terrorism 33(7), 652-671, p.660
[117] Kaurnerts [n124] p. 661
[118] [n113] p.304

fight against terrorism.[119] This could help to explaining why both amongst EU Member States and the EU with third countries there is that reluctance to share fully terrorism related intelligence.

The Relationship between EU Member States' Security Agencies and Europol

The second problem exists in relation to Member States' attitude towards sharing intelligence with Europol is the lack of an obligation on Member States' national security agencies to co-operate. One issue potentially underpinning this problem is Member States could see this as ceding further sovereignty to the EU on issues traditionally dealt with by nation states. This could explain why some Member States have been reluctant to give the EU further powers on dealing with terrorism, especially in relation to intelligence exchange as they see the EU interfering with Member States' existing laws, national security practices and relationships with third countries.[120] Muller-Wille notes as national counter-terrorism agencies will be judged and held accountable for their success against international terrorism to their own Member State Government and that state's citizens, those agencies, '…cannot and will not rely on Europol's contribution'.[121] Even during the Lisbon Treaty negotiations a large number of Member States, in particular the UK and France successfully insisted that intelligence matters should remain outside the realm of the integration process. As Coolsat observes, the UK was able at the eleventh hour to insert into the Lisbon Treaty in article (4.2) that national security which includes the governance of the intelligence services remains the sole responsibility of each Member State. Article 4.2 states:

> 'The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the

[119] [n123] p.69
[120] [n119, p.129
[121] [n123] p.57

> State, maintaining law and order and safeguarding national security. *In particular, national security remains the sole responsibility of each Member State*.' [my emphasis]

In trying to pin down the key rationale behind this thinking could be the role of intelligence. The problem for Europol is it is seen as a policing not a security agency. These two agencies see and use intelligence differently with the police tending to use intelligence to gain information and evidence on targets they are about to arrest whereas security agencies are interested in intelligence to profile individuals and group that pose a threat to security without prosecutorial purposes.[122] This is crucial point as it could be the EU's data protection laws that is an inhibiting factor in Member States wanting to involve their national security/intelligence agencies in co-operation with the EU, especially Europol. As Muller-Wide notes, legislation protecting civil liberties does not allow security services to intrude into the private space of citizens.[123] Commenting on this issue Kaunert and Leonard say that if the EU became more flexible on the issue of data protection this could pave the way to increased police and law enforcement co-operation in counter-terrorism,[124] even increased co-operation between EU Member State national security/intelligence services.

Accountability of Europol and the Rule of Law

There is a reason to be optimistic about future developments in the role of Europol and terrorism related intelligence exchange and these come from the changes to the legal instruments governing Europol. These changes regarding Europol's role are important for two reasons that centre on accountability. Firstly, through the hierarchy of agencies associated with the EU's Justice and Home Affairs Commission, Europol has a vertical legal legitimacy that is identifiable when compared the horizontal role of agencies made under the

[122] Oldrich Bures (20130 'Europol's Counter-Terrorism Role: A Chicken-Egg Dilemma' in Christian Kaunert and Sarah Leonard (editors) European Security, Terrorism and Intelligence: Tackling new Security Challenges in Europe London: Palgrave 65-95, p.72
[123] [n123] p.65
[124] [n113] p.295

multi-lateral agreements.[125] This is important regarding accountability as the ToL provisions brings Europol under the jurisdiction and scrutiny of the ECJ. The second reason why this development is important concerns the actions of Europol within the legal principle of the rule of law. As Europol's actions can be scrutinised by the ECJ as well as the EU Parliament:

> 'The constitutive role of the rule of law relates to the means by which the community is governed: through law. The law regulates social relationships and therefore effective enforcement of the law is constitutive for the rule of law'.[126]

This is important as such accountability would satisfy intelligence gathering and exchange is operating within a legal framework balanced by the law governing rights to privacy and data protection.

In its desire to ensure it can be an effective international actor, the EU's counter-terrorism measures in particular have led to an increased divergence of Member States' law that can be achieved by replacing the framework decisions with regulations and directives that are more effective.[127] Supporting this and the Treaty of Lisbon has been the Stockholm Programme[128] mapping out the 2010-2014 plan to provide an open and secure Europe, serving and protecting citizens.[129] This programme stresses that EU criminal law and counter-terrorism measures will be pursued on the basis of the constitutional arrangements brought into place by the Treaty of Lisbon. This includes co-operation in the collection, storage, processing, analysis and exchange of relevant information between EU Member State competent authorities.[130] The rationale for this, as Murphy's study recognised, is with the

---

[125] [113] p. 106
[126] Cain Murphy (2012) *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* Oxford: Hart Publishing, p.35
[127] Ibid p255
[128] 2010/C 115/01
[129] The UK's House of Lords is already calling for input to the JHA's next five year agenda that is likely to be the Rome Plan http://www.parliament.uk/business/committees/committees-a-z/lords-select/eu-home-affairs-sub-committee-f-/news/rome-cfe/ [accessed 3rd September 2013]
[130] Treaty of Lisbon, article 87.2(a)

volume of EU criminal law and counter-terrorism measures is set to increase in the coming years[131] it will require stricter adherence to mutual co-operation between the Members States and Europol as well as enhancing the reputation and reliability of Europol's role as an international actor with Member States and third countries. One way forward would be moving from the traditional stance of the intelligence and police community regarding intelligence exchange to move from a need to know basis to a need to share.[132] The advantages of moving to a sharing culture regarding terrorism intelligence is as Occhipinti points out it emphasises the responsibility to provide where intelligence data is unlocked from a fragmented technology infrastructure spanning multiple intelligence agencies and make intelligence readily discoverable and accessible from the earliest point at which an analyst can add value.[133] With the main aim of any counter-terrorism activity is to prevent acts of terrorism occurring thereby protecting the right to life of citizens and with the threat of international terrorism increasing the potential for terrorist activity this is the most logical way to go forward in countering terrorism.

Recommendations

PNR Directive

While the Directive 2012/0010 (COD) is expansive in its coverage of criminal activity it is submitted that a separate directive is required to deal with the transfer of PNR. Building on the 2011 draft PNR Directive, a new draft text on an EU system for the use of PNR data was tabled by lead Member of the European Parliament (MEP), Timothy Kirkhope (ECR, UK) that was discussed in the LIBE Committee on 26 February 2015. An evaluation of the necessity and proportionality of the proposal in the face of current security threats, its scope (list of offences covered), retention periods, the inclusion or exclusion of intra-EU flights, the

[131] [n126] p.241
[132] [115] p.70
[133] John Occhipinti (2013) 'Availability by Stealth? EU Information-sharing in Transatlantic Perspective' in Christian Kaunert and Sarah Leonard (editors) *European Security, Terrorism and Intelligence: Tackling new Security Challenges in Europe* London: Palgrave 143-184, p.152

connection with the on-going data protection reform, as well as the consequences of the EU Court of Justice judgement annulling the 2006 data retention directive, were among the issues discussed by MEPs. The 2011 Commission proposal would require more systematic collection, use and retention of PNR data on passengers taking “international” flights (those entering the EU from, or leaving it for, a third country), and would therefore have an impact on the rights to privacy and data protection.

The changes proposed by Timothy Kirkhope in the revised draft report include:

- The scope of the proposal is narrowed to cover terror offences and serious "transnational" crime (the list of specific offences includes, for instance, trafficking in human beings, child pornography, trafficking in weapons, munitions and explosives);
- Sensitive data to be permanently deleted no later than 30 days from the last receipt of PNR containing such data by competent authorities. Other data will continue to be masked after 30 days;
- The inclusion of intra-EU flights (not initially included by the Commission, but the Council of the European Union favours the inclusion of internal EU flights);
- 100% coverage of flights (the Commission text proposed to reach 100% coverage of international flights in gradual steps);
- Access to the PNR data continues to be allowed for five years for terrorism, but is reduced to four years for serious crime;
- Each EU Member State should appoint a data protection supervisory officer;
- Persons who operate security controls, who access and analyse the PNR data, and operate the data logs, must be security cleared, and security trained;
- References are made in the text to the EU Court of Justice judgment on data retention and to the current EU data protection rules; and,
- The period for member states to transpose the directive is extended from two to three years (given the specific technological and structural demands of setting up an EU PNR system for each member state).

It is understandable why the revised draft included serious transnational crime as well as terrorism as offences such as the trafficking of human beings causes great suffering to those who are being trafficked. However, the trafficking in weapons, munitions and explosives can be linked to terrorism investigations. The wider the inclusion of offences thereby giving greater access to PNR data, there is the potential for wider data mining and profiling of EU citizens. The advantage of linking PNR data access to terrorism investigations minimises

potential abuse in the collection and retention of PNR data. By having tighter control in the data's access by only allowing security and counter-terrorism policing agencies to use the data to link passenger connections with known terrorist or terrorist organisations currently on intelligence systems again minimises the potential for offender profiling.

Incorporating some of the points in the revised draft and building on it, it is submitted that consideration be given to the following points, which is more likely to conform to data privacy and protection law and avert fears of a surveillance society. While keeping from Kirkhope's revised draft that each EU Member State appoint a data protection supervisory officer, persons who have access to PNR data are security cleared and have training, and, that in the Directive reference is made to EU Court of Justice and current EU data protection rules, a PNR Directive proposal includes:

- Any amended Directive is solely related to terrorism investigations;
- The Directive only applies to targeted flights to and from states that border or are terrorist conflict zones;
- The PNR data is only held by competent authorities (who would be Member States' national security agencies and Counter-Terrorism Policing Departments);
- Requests for PNR data on applicable flights is carried out through and by Europol on behalf of the respective Member State competent authority requesting the data;
- It is necessary that all Member States collect, process and exchange PNR data to avoid security gaps as this will contribute towards the security of the EU;
- All PNR data is handled in accordance with the provisions of Article 8 of the Charter of Fundamental Rights of the European Union, Article 16 of the Treaty on the Functioning of the European Union and article 39 treaty for Union along with article 8 ECHR;
- The data is pulled from the PNR data solely for matching purposes in relation to terrorism intelligence already in the possession of the Member States' competent authorities. The data cannot be requested for sole purpose offender profiling, thereby preventing data mining.

In addition to these suggestions, the sections in Kirkhope's revised draft referring to serious crime is omitted and by targeting flights to or states bordering terrorist conflict zones rather than all flights, this reduces the concern over data mining by Member States' competent authorities. The flights that are targeted will be based on intelligence,

in particular those recognised by Europol from its intelligence source, Schengen Information System II. This targeting could be fluid to match travel patterns as countries are identified as destinations for those wanting to travel and join terrorist groups. The main aim of counter-terrorism investigations is to prevent terrorist acts from happening and ensuring that EU Member States' citizens are safe. Such a proposal would enhance this capability and it is submitted this proposal is not only necessary but is also a proportionate legislative response to the terrorist threat the EU faces.

Surveillance of Electronic Communications Data Directive

The proposals for a new Surveillance of Electronic Communications Data Directive include:

1. Relevant Member State's Secretary of State issue an order to ensure that communications data from ISP and CSP's is obtained and made available to relevant public authorities (in particular national security and counter-terrorism policing agencies) or to facilitate the availability of communications data to be obtained from ISP and CSP's;
2. Such an order will provide for the obtaining by ISP and CSP's of communications data, the processing, retention or destruction by ISP and CSP's they obtain or hold. Processing here includes the methods used by ISP and CSP's in its reading, organisation, analysis, copying, correction, adaption or retrieval and integration with other communications data;
3. The order to impose requirements in ISP and CSP's to ensure the communications data is disclosed without undue delay, to comply with the order while respecting rights to privacy and data protection;
4. Impose safeguards in relation to ensuring the order is necessary in a democratic society and is proportionate to the threat the Member State is facing and complies with the qualifications to interfere with the right to an individual's privacy as well as complying with data protection law. This can be achieved by judicial scrutiny by a member of the respective Member State's senior court (on behalf of the ECJ) with assistance from Eurojust;
5. As part of the safeguards, the ISP or CSP can apply via Eurojust to the senior judiciary of the Member State making the order where the operator considers the order is neither necessary and proportionate, and does not comply with rights to privacy and data protection;
6. Any communications data forwarded onto the relevant Membered State public authority is retained for a maximum of 12 months to allow that authority to analyse the data with their respective intelligence systems related to terrorism activity in order to make any connections with those individuals or groups that have been identified as a threat and whose activities are already subject of

lawful surveillance. This is also to allow for co-operation with third countries' agencies involved in monitoring terrorist activity outside the EU regarding intelligence analysis. This can be carried out with the guidance of Europol;

7. ISP and CSP's destroy communications data requested by an order when that data is no longer authorised for retention by the order in a way it cannot be retrieved;
8. Interception warrants – where a person or a group has been identified by a Member State's national security or counter-terrorism policing agency as being involved in terrorist activity the relevant Member State's Secretary of State my authorise an interception of communications warrant (that includes that person or group's use of electronic communication via social media sources) where it is necessary and proportionate to do so in the interests of national security or to prevent or detect crime and disorder;
9. Europol collate all interception warrants so issued and assist the Member State public authority by analysing the intelligence assessing potential connections with terrorism related intelligence obtained from other Member states and third countries;
10. Safeguards for interception warrants could include verification the warrant is lawful by senior members of the Member State's judiciary, assisted by Eurojust;
11. Communications data obtained via an interception warrant is retained for a period of 12 months. Where the communications data is forming evidence of an ongoing investigation that data can be retained longer when it is believed necessary to form part of the evidence is any potential criminal trials that may result from that investigation.

Conclusion

Following the Snowden revelations in 2013 regarding the electronic surveillance practices of the US' NSA and the UK's GCHQ, it is understandable there is a degree of caution when legislation is considered in granting further surveillance and data gathering powers to national security and policing agencies. This is certainly the situation for EU bodies when it was revealed that EU Member State leaders and citizens were targeted by the NSA and GCHQ. As outlined, the terrorist threat is a constantly evolving issue and the current threat, especially from Islamist terror groups is severe. In just the early months of 2015 EU Member States have suffered the devastating effects of terrorist attacks in Paris (January 2015) and Copenhagen (February 2015). This is in addition to the Member States counter-terrorism agencies, supported by Europol, preventing terrorist attacks during this period. When senior figures of security and policing agencies are openly expressing their concerns over their

respective agency's capability to consistently prevent attacks under the current surveillance related legal framework, these expression should not be ignored. As covered, with the ever increasing number of EU citizens flying to or returning from countries bordering states containing Islamist terror groups' bases, an introduction of a PNR Directive would go some way to aid security and counter-terrorism policing agencies in identifying individuals who may pose a security threat. In addition to the proposals for the data protection Regulations and Directives that will be introduced in 2016, the EU already has in place legal provisions to protect personal data. The recommendation submitted here of a new PNR Directive that is applicable only to terrorism related activity, along with minimal data retention and intelligence analysis linked to suspects already on intelligence systems would help to protect personal data as well as going some way to aiding those agencies' investigations into acts of terrorism. Enhancing the capability of preventing terrorist acts enhances further EU Member States' agencies capability of protecting EU citizens, especially in protecting their right to life. The right to life is just as important as the right to privacy.