‘The Terrorist Threat Facing EU Member States: Time for the EU to introduce a Directive on Electronic Surveillance in Terrorism Investigations to Plug the Security Gap’

David Lowe

Liverpool John Moores University

Law School

Brownlow Hill

Liverpool L3 5UG

UK

Email: D.Lowe@ljmu.ac.uk

Tel No: 0151 231 3198

Introduction

The use electronic communications by terrorist groups is an international concern to many states including the EU Member States. This concern centres mainly on how communications are used to radicalise citizens resulting in them either leaving their home state to join and fight with terrorist groups in conflict zones or in encouraging citizens to take up the cause and carry out attacks in their home state. With the various forms of electronic communication used, especially the various social media sources, intelligence and counter-terrorism policing agencies are claiming they are struggling to carry out effective surveillance on targets as they try to prevent attacks from occurring. They claim this is resulting in a security gap.

By looking at the terrorist threat the EU is currently facing and the clamour for wider surveillance powers, this paper considers the concerns of the surveillance society, especially following the revelations by Edward Snowden in the activities of the US' National Security Agency (NSA) and UK's General Communications Headquarters (GCHQ). The main concern centres on the lack of protection of rights to privacy and data protection as states attempt to protect the interests of national security. By examining the communications data that is subject of surveillance this paper looks at the surveillance legislation recently passed or is proposed in France, Canada, the UK and the US considering the similarities in the issues the legislation raises regarding plugging the security gap as well as concerns surrounding the lack of data protection contained in this legislation.

This paper proposes that as rights to privacy and data protection is deeply embedded into its law, the EU is ideally placed to take the lead in gaining the co-operation of Internet and Communications Service Providers. This includes a recommendation that now is an opportunity for the EU to introduce legislation to be adopted in its twenty-eight Member States that will provide sufficient powers of surveillance in protecting the interests of national

security while protecting rights to privacy and data protection. This recommendation includes an analysis of the EU's laws on data protection including the important decision in the *Digital Rights* case.

The Terrorist Threat to the EU

The civil war in Syria and the control of large parts of Iraq by Islamic State has allowed a vacuum to exist enabling Islamist groups, in particular Islamic State (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 pose a threat to the security of the Syrian/Iraqi region and to the security of nations around the world, including EU Member States. The threat is posed on two fronts. Firstly the number of citizens from nation states outside Syria and Iraq who have gone to these countries to join Islamist terror groups. In January 2015 from two EU Member States it is estimated that 600 UK citizens and 1,500 French citizens have travelled to Syria to join Islamic State.[1] A major concern for EU Member States is those returning from conflict zones who see their home state as an enemy resulting in these citizens being more likely to plan and carry out terrorist attacks in their home state. The second threat is in how these terrorist groups' skilful use of electronic communications, in particular social media, in radicalising EU citizens and influencing them either join these groups in the conflict zones or to carry out terrorist attacks in their home EU Member State.

This alarming increase in the number of citizens who have gone to Syria and Iraq to fight with Islamic state has led to Europol's Director, Rob Wainwright, 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. His concerns centre on the difficulties the security and

[1] 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]

policing agencies are currently facing in monitoring electronic communications used by terrorists. Wainwright said that hidden areas of the Internet and encrypted communications are making it harder to monitor terrorist suspects, adding that Tech firms 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.[2]

In September 2014 three Dutch citizens were arrested in the Netherlands 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.[3] Even where there are small numbers, the danger of having Islamic State followers in the EU's Member States was evident in May 2014 when four people were killed at the Jewish Museum in Brussels[4] by an Islamic State militant, Muhdi Nemmouche.[5]

On January 7th 2015 Europe received a stark wake-up call as the threat Islamist groups pose with the attack on the offices of the French satirical magazine, Charlie Hebdo where Cherif and Said Kouachi killed twelve people, ten of the magazine's staff and two police officers who were protecting the building. These two brothers were French citizens of Algerian descent who were influenced by Al Qaeda,[6] where the Al Qaeda affiliate, Al Qaeda

[2] 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]
[3] 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]
[4] 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]
[5] 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]
[6] 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]

in the Arabian Peninsula (AQAP) claimed responsibility for the attack.[7] 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, killing four of the hostages before the French police stormed the building killing Coulibaly.[8] Both he and the Kouachi brothers were killed by the French police following two respective siege situations.[9] 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. Using social media sources, he faked his own death in an attempt to return to the UK.[10] In January 2015 Andrew Parker, the head of the UK's intelligence agency MI5 pointed out that under current legal conditions trying to monitor the sophisticated use of electronic communications by terrorist group, it is virtually impossible to prevent every type of attack.[11]

Concerns over the Surveillance Society: The Snowden Revelations

Granting intelligence and policing agencies wider surveillance powers generates fears of a surveillance society. In 2013 those fears were confirmed following the revelations by the

[7] 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]
[8] 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]
[9] 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]
[10] 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]
[11] Security Service MI5 (2015) 'Address by the Director-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]

former NSA employee, Edward Snowdon on the practices of the NSA and GCHQ in relation to Operation PRISM .[12] 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, Microsoft, Facebook, Yahoo, Skype and Apple.[13] 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'.[14] 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.[15] 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

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

[13] 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]

[14] 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]

[15] 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]

were passed onto the UK's security agencies, MI5, MI6 and Special Branch's Counter-Terrorism Unit.[16]

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.[17] 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.'[18]

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.[19] 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.[20] 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. While understanding the concerns of a surveillance society, 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.

---

[16] 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]
[17] Ibid p.141
[18] Ibid p.142
[19] Murphy, C.C. (2012) EU Counter-Terrorism Law: Pre-Emption and the Rule of Law Oxford: Hart Publishing, p.149
[20] Whitman, J.Q. (2004) The Two Western Cultures of Privacy: Dignity versus Liberty 113 *Yale Law Journal* 1151—1221, p.1155

UK Liberty Civil Liberty Groups' Concerns Regarding Widening Surveillance on Electronic Communications Data

In March 2015 the UK's Intelligence and Security Committee of Parliament (ISC) published is report on privacy and security. By being developed piecemeal, the ISC found the UK's legal framework regarding surveillance, especially on electronic communications is unnecessarily complicated raising concerns over a, '…lack of transparency, which is not in the public interest.'[21] As a result, among its recommendations is that all the current legal frameworks on surveillance are replaced with a new Act of Parliament.[22] In this recommendation the ISC stated that as human rights obligations can constrain surveillance practices they emphasised the requirement for transparency and reporting when such powers are used.[23]

Surprisingly the ISC's findings have not been universally welcomed. The UK civil liberties group, Liberty have no confidence in the ISC's ability to, '…provide effective oversight of the security agencies'.[24] Underpinning this claim is Liberty's perception that by being understaffed and under-funded the ISC has insufficient expertise, which leads them to consistently fail to criticise the UK's intelligence. Liberty say the ISC act more like, '…a spokesperson of the agencies than a credible oversight body.'[25]

When members of four UK privacy campaign groups gave evidence to the ISC's inquiry into privacy and security, the ISC asked them if evidence emerged through bulk data collection terrorist attacks were being prevented, would they still believe so strongly that under any circumstances bulk data collection is so unacceptable that terrorist attacks is a price a free society has to pay. The four privacy campaigners said it was with Isabella Sankey, the

[21] Intelligence and Security Committee of Parliament (2015) 'Privacy and Security: A modern and transparent legal framework' London: Her Majesty's Stationary Office, p/2
[22] Ibid p. 118
[23] Ibid pp.118-119
[24] 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
[25] Ibid, p.4 paragraph 5

director of policy of the Liberty saying, 'Yes …That is the price you pay to live in a free society.'[26] 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'.[27] For some this response may appear astounding and irresponsible while for others this stance is plausible. This shows how polarised views are on practises related to surveillance of electronic communications that gathers bulk data collection. This could be due to the nature of the communications that comes under legislation related to surveillance and data retention.

The Communications Data Subject of Wider Surveillance

The electronic communications data subject in many states' recent and proposed legislation granting further powers of surveillance includes communication data that details of the time, duration, originator and recipient of communication. In common parlance this is, 'the who, when and where of communication, but not the content of the communication itself'.[28] Breaking it down to three distinct categories, communications data includes:

1. Traffic Data –where communications are 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 Internet Service Provider (ISP) or Communications Service Providers (CSP) where the information is about the person using the service provided by the ISP or CSP.

[26] Intelligence and Security Committee of Parliament (see note 47) pp. 35-36
[27] Ibid p.36
[28] Simon McKay (2015) 'Covert Policing: Law and Practice' (2nd edition) Oxford: Oxford university Press, p.129

> 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[29]

This is bulk data and while not being able to see the content of communications, it allows intelligence and policing agencies to trace and acquire information on the movements of a person. It is essential that in allowing such agencies to carry out surveillance on electronic communications data that stringent controls are in place protecting privacy and data protection.

Recently passed and proposed legislation widening surveillance of electronic communications data

France

On the 5th May 2015 the lower house of the French National Assembly adopted a Bill on intelligence-gathering that is expected to come into effect as law in early July 2015.[30] The key provisions in the Bill include:

1. Without judicial scrutiny or authorisation, it is granting authorities for French intelligence services to conduct surveillance on digital and mobile phone communications. This includes forcing ISP and CSP to give up data upon request;
2. Intelligence services the right to place cameras and recording devices in private homes and install key-logger devices that are capable of recording every key stroke on a targeted computer in real time;
3. Intelligence services can 'vacuum up' bulk data that will be subject to analysis for 'potentially suspicious behaviour. While the bulk data will remain anonymous, intelligence agents could apply for a request to an independent panel for deeper surveillance to yield the identity of users;
4. ISP and CSP's install complex algorithms that will flag up suspect behavioural patterns online such as key words used, site visits and contacts made;
5. Authorities will be able to keep recording for one claender month and bulk data for five years.[31]

Under the Bill, surveillance authorities can be granted where the surveillance is required in a terrorism investigation or is deemed necessary to protect national independence, territorial

[29] 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

[30] Soeren Kern (2015) 'French Parliament Approves Sweeping Surveillance Law' Goldstone Institute retrieved from http://www.gatestoneinstitute.org/5703/france-surveillance-law [accessed 3rd June 2015]

[31] Angelique Chrisafis (2015) 'France passes new surveillance law in wake of Charlie Hebdo attack' *The Guardian* 5th May 2015 retrieved from http://www.theguardian.com/world/2015/may/05/france-passes-new-surveillance-law-in-wake-of-charlie-hebdo-attack [accessed 3rd June 2015]

integrity and national defence. The grounds under which a surveillance authority is granted has been criticised by the head of the Paris Bar Association, Pierre-Oliver Sur who said:

> 'We cannot accept a law that notably authorises the establishment of systems that not only locate people, vehicle or objects in real time, but also capture personal data, based on what the drafters of the law call, vaguely "the major interests of foreign policy", "the economic, industrial and scientific interests of France", "the preventions of collective violence" or "the prevention of crime and organised crime"[32]

As with most pieces of legislation granting surveillance powers, to ensure the laws relating to privacy and data protection are complied with, the Bill contains safeguards. To ensure the powers are not abused or used inappropriately surveillance authorities will be scrutinised by the National Commission for Control of Intelligence Techniques (CNCTR). The CNCTR will consist of a nine-person committee led by the French Prime Minster. These safeguards have not escaped criticism. The main criticism is the creation of the CNCTR removes any scrutiny of authorities' surveillance practise by the judiciary. It is argued this move does not fit in a true democracy where state agencies should be governed by the rule of law. True impartiality can only be through the judiciary, as judges are suitably placed to decide if there should be restrictions of fundamental freedoms.[33] Liberty and privacy groups say the establishment of the CNCTR is meaningless as it has not been invested with any real power because its remit is limited to providing the French Prime Minister with non-binding advice and the CNCTR cannot overrule the Prime Minister. Even though the CNCTR can refer concerns they have to France's highest administrative court, the Council of State which does have power to end surveillance, CNCTR's oversight is illusory with the Bill effectively

[32] [n25]

[33] Mike Woods (201)0 'France's new spy bill raises fears of mass surveillance' RFI 13th April 2015 retrieved from http://www.english.rfi.fr/france/20150413-france-s-new-spy-bill-raises-fears-mass-surveillance [accessed 3rd June 2015]

centralising power to the hands of a few individuals.[34] The online advocacy group La Quadrature du Net wrote argue that:

> 'Representatives of the French people have given the Prime Minster the power to undertake massive and limitless surveillance of the population. By doing so, they're ensuring that the power of the state and the basis of our democratic system are getting ever more distant.'[35]

Canada

Also on the 5th May 2015, Canada was passing its Anti-Terrorism Act 2015. Key provisions include:

1. Part 1 of the Act is concerned with information sharing between the government of Caned institutions in order to protect Canada against activities that undermines the security of Canada, provided the information sharing is consistent with the Canadian Charter of Rights and Freedoms;[36]
2. Part 2 of the Act is aimed at securing air travel where the Minister can establish a list of persons who they have reasonable grounds to suspect a person's actions that comes under the definition of terrorism in section 83.2 of the Criminal Code engages or attempts to engage in an act that threatens transportation security or travels by air for that purpose.[37] The Minister can delegate this power to employees of the Department of Public Safety and Emergency Preparedness.[38] Those who can assist in the collation of such a list include the Minister of Transport, Minister of Citizenship and Immigration, member of the Royal Canadian Mounted Police, the Director of the Canadian Secret Intelligence Service and an employee of the Canada Border Services Agency.[39]
3. Part 3 of the Act makes amendments to the Canadian Criminal Code where key amendments in relation terrorism includes introducing an offence of advocating or promoting commission of terrorism offences where a person commits an offence if they communicate statements, knowingly advocate or promote the commission of terrorism offences in general knowing that any of those offences will be committed or are reckless as to whether they are committed will commit an offence that liable to imprisonment;[40]
4. Another key amendment is an amendment to code 83.233 of the Canadian Criminal Code relating to terrorist propaganda or computer data that makes terrorist propaganda available to the public through a computer system where the amended s.83.223(5) of the Criminal Code states that if the court is satisfied that on the balance of probabilities that the material is available to the public and is terrorist propaganda

[34] [n.25]
[35] BBC News (20150 'French parliament approves new surveillance rules' 6th May 2015 retrieved from http://www.bbc.co.uk/news/world-europe-32587377 [accessed 3rd June 2015]
[36] S.3 of Security of Canada Information Sharing Act contained in Anti-Terrorism Act 2015
[37] S.8 Secure Air Travel Act contained in the Anti-Terrorism Act 2015
[38] S.7 Secure Air Travel Act contained in the Anti-Terrorism Act 2015
[39] S.10 Secure Air Travel Act contained in the Anti-Terrorism Act 2015
[40] S.16 Anti-terrorism Act 2015 that amends section 83.221 of Canadian Criminal Code

> or computer data that makes terrorist propaganda available, the court may order the computer system's custodian delete the material.

In addition to the court making the orders giving judicial scrutiny of the Act's provisions, another safeguard contained in the Act is a requirement of the Canadian Security Intelligence Review Committee to provide oversight of the Canadian Secret Intelligence Service and report on any disruption activities that take place under the Act.

The Act has been subject to criticism where campaigns to stop the Act becoming law were formed. One of the campaigns was a Twitter campaign, #VoteAgainstC51 where the author, Margaret Atwood, saw the Act attacking Canadian rights and freedoms. She urged Canadian Members of Parliament to 'do the right thing' and vote against the Act.[41] Further criticism came from the Privacy Commissioner of Canada, Daniel Therrien who said:

> 'The scale of information sharing proposed is unprecedented, the scope of the new powers conferred by the act is excessive, particularly as these powers affect ordinary Canadians, and the safeguards protecting unreasonable loss of privacy are seriously deficient. All Canadians would be caught in this web.'[42]

United Kingdom

Following the Conservative Party's 2015 General Election victory, the Queen's Speech outlining the legislation the new UK Government would introduce during the 2015/16 Parliament was delivered on the 27th May 2015. The UK Government proposes to introduce the Investigatory Powers Bill giving UK intelligence and policing agencies greater powers to monitor Internet and telephone use. The UK Government claim the Bill will address the gaps in intelligence gathering and enable the agencies to access communications data that is putting lives at risk, saying it will provide the authorities with the, '…tools to keep you and

[41] John Barber (2015) 'Canada poised to pass anti-terror legislation despite widespread outrage' *The Guardian* 5th May 2015 retrieved from http://www.theguardian.com/world/2015/may/05/canada-anti-terror-law-despite-widespread-protest [accessed 25th May 2015]
[42] Ibid

your family safe.'[43] A UK Government document says the purpose of the Investigatory Powers Bill will be to:

1. Address ongoing capability gaps that are severely degrading the ability of law enforcement and intelligence agencies ability to combat terrorism and other serious crime;
2. Maintain the ability of UK intelligence agencies and law enforcement to target the online communications of terrorists, paedophiles and other serious criminals;
3. Modernise the UK's law in the areas of terrorism and serious crime and ensure it is fit for purpose;
4. Provide for appropriate oversight and safeguard arrangements.[44]

The UK Government claims this Bill will enable the intelligence services and police to meet their operational requirements by addressing the gap in their ability to build on intelligence and evidence where suspects have communicated online.

UK civil liberty groups are concerned the impact the Bill will have on rights to privacy and data protection. Jim Killock from Open Rights Group sees the Bill as signalling the UK Government's desire to press ahead with increased powers of data collection and retention, allowing the police and GCHQ to spy on everyone whether or not they are suspects of committing a crime or not, adding:

> 'We should expect attacks on encryption, which protects all our security. Data collection will create vast and unnecessary expense'[45]

Renate Samson from Big Brother Watch is sceptical if there is a security gap questioning if there is any real evidence of a gap in the capability of law enforcement and intelligence

[43] BBC (2015) 'Queen's Speech: New monitoring powers to tackle terrorism' 27th May 2015 retrieved from http://www.bbc.co.uk/news/uk-politics-32896921 [accessed 28th May 2015]
[44] Gov.UK (2015) 'Queen's Speech 2015: what it means for you' 27th May 2015 retrieved from https://www.gov.uk/government/publications/queens-speech-2015-what-it-means-for-you/queens-speech-2015-what-it-means-for-you#investigatory-powers-bill [accessed 28th May 2015]
[45] [n.38]

agencies' ability to gain access to communications data. She said, 'Any new draft legislation must acknowledge that the bigger the haystacks the harder it will be to find the needles.' [46]

At the moment one can only guess the Bill's contents, but it could be similar to the Communications Data Bill presented to the UK Parliament in June 2012 during the 2010-2015 Coalition Government that was blocked by the Liberal Democrat members of the Coalition who saw the proposed measures being too intrusive.[47] The most controversial points in the Communications Data Bill were under the following clauses. Clause 1 proposed to give the relevant Secretary of State power to issue an order to ensure that communications data is made available to the appropriate authorities by ISP and CSP's. Clause 4 regarding the period the ISP and CSP's must retain the data. Clauses 5 and 9 regarding authorisation to and access to data by the intelligence and policing agencies, where Clause 9 proposed that ISP and CSP's disclose the details of persons those agencies suspected to be involved in terrorism or serious criminal activity provided it was necessary and proportionate to do so, where among a number of reasons listed, those grounds included:

1. Where it is in the interests of national security;
2. To prevent or detect crime or of preventing disorder;
3. Where it is in the interests of the economic well-being of the UK;
4. Where it is in ten interests of public safety

One can see that these grounds are the qualifications listed in article 8 (Right to Privacy and Family Life) European Convention on Human Rights. It is expected that similar clauses will be contained in the Investigatory Powers Bill.

[46] Renate Samson (2015) Reaction to the Queen's Speech – Investigatory Powers Bill retrieved from https://www.bigbrotherwatch.org.uk/media-and-press/reaction-to-the-queens-speech/ [accessed 28th May 2015]
[47] [n.38]

United States

On the 2nd June 2015 Congress passed the Freedom Act 2015. This Act amends the Foreign Intelligence Surveillance Act 1978 (FISA), effectively replacing the amendment provisions to FISA by the Patriot Act 2001, mainly affecting section 215 FISA. The Act also covers the retention of communications data by US federal agencies, in particular the NSA. The Act was introduced following the US President Barak Obama's promise to change FISA following the Snowden revelations. Also influential in legislative changes being introduced were judicial challenges to the Patriot Act amendments to FISA in the US courts. In 2015 the case *American Civil Liberties Union (ACLU) and others v Clapper and others*[48] went before the United States Court of Appeals for the Second Circuit. The Court followed the approach taken by US District Court for the District of Columbia in *Klayman et al v Obama and others*[49]where the District Court stayed the applicants' injunction and ordered the NSA to terminate its bulk data collection. In *ACLU v Clapper* the ACLU's claim was the NSA's metadata collection programme exceeded the authority granted to them by the Foreign Intelligence Surveillance Courts (FISC). The Court of Appeals held that as the applicants had shown there was a degree of certainty that their telephone use was under a FISA authority and this was illegal depriving the applicants of their constitutional rights.[50] At the time of making their decision the Court did recognise section 215 FISA was scheduled to expire and that Congress were to debate the Patriot Act's sunset clause.[51] In reaching their decision, the Court said:

> 'This case serves as an example of the increasing complexity of balancing the paramount interest in protecting the security of our nation – a job in which, as the President has stated, "actions are second guessed, success in unreported, and failure can be catastrophic." …Reconciling the clash of these values [national

[48](2015) Case 14-42
[49] (2013) Civil Action Number 13-0881 (RJL)
[50] Ibid p.94
[51] Ibid p.96

> security and rights to privacy] requires productive contribution from all three branches of government, each of which is uniquely suited to the task in its own way.'[52]

Among the key changes the Freedom Act 2015 make to FISA includes a prohibition of bulk data collection where the collection now has to be targeted to a specific section term. A specific selection term is defined as that, '…specifically identifies a person, account, address, or personal device or any other specific identifier.'[53] The Act makes it clear a specific identifier does not include an identifier that has no limit to the scope of information sought and cannot be a method of surveillance gathering unless the provider is subject of an authorised investigation for which the specific selection term is used as the basis for the use.

Regarding unlawfully obtained information a court can order a correction of a deficiency, but no information or evidence so derived and certified by the court as being deficient concerning a US citizen can be received as evidence in any trial, hearing or other court proceeding except with the approval of the Attorney General where that information indicates a threat of death or serious bodily harm to a person.[54] The Act also guarantees greater transparency of the decision making of the FISC, whose hearings have been *in camera*. The Act requests declassification of the FISC's decisions, orders and opinions are carried out to make publically available to the 'greatest extent' practicable,[55] but where necessary they can be released in a redacted form.[56]

Responses to the Act have been mixed. Acknowledging the Freedom Act is a historic step forward, Neemah Guiliani, the ACLU legislative counsel, said the Act is not as strong as they wanted and would like to see the following reforms:

[52] Ibid pp.96-97
[53] s.201(b) Freedom Act 2015
[54] s.301 Freedom Act 2015
[55] s. 602(a) Freedom Act 2015
[56] s. 602(b) Freedom Act 2015

1. Urge the US President and Congress to rein in surveillance orders used to collect information about millions of Us citizens absent from any judicial process;
2. Add a reform to FISA which allows the government to collect the content of Americans' communications with individuals abroad;
3. Reject efforts to expand surveillance through cybersecurity information-sharing legislation.[57]

The Senator for Minnesota, Al Franken, described the Freedom Act a measured compromise legislation that is the result of lengthy negotiations that bring much needed reform to the issuing of authorities saying in relation to the declassification of FISC decisions:

> '[The Act] strikes a balance that we need, but of course the public can't know if we are succeeding in striking that balance if they don't have access to even the most basic information about the surveillance process.'[58]

Not all Congress senators see the Freedom Act as striking a balance between the needs of national security and the protection of privacy. For the Kentucky Senator, Mitch McConnell the Act undermines national security. During the Act's passage through Congress he said, 'To dismantle our counterterrorism tools [the president has] not only been inflexible [but also] extremely ill-timed' adding that Snowden handed a 'playbook' to Islamic State and Al Qaeda the scope of NSA surveillance programmes, saying:

> 'Our nation has a regrettable history of drawing our forces and capabilities only to find ourselves ill prepared for the next great struggle. … [The Freedom Act] is ending the tools created by the previous administration to wage the war on terror.'[59]

[57] Neema Guiliani (2015) 'What's Next for Surveillance Reform After the USA Freedom Act' retrieved from https://www.aclu.org/blog/washington-markup/whats-next-surveillance-reform-after-usa-freedom-act [accessed 3rd June 2015]
[58] Alan Yuhas (2015) 'NSA reform: USA Freedom Act passes first surveillance reform in decade' *The Guardian* 2nd June 2015 retrieved from http://www.theguardian.com/us-news/live/2015/jun/02/senate-nsa-surveillance-usa-freedom-act-congress-live [accessed 3rd June 2015]
[59] Ibid

Similarities in Issues Between the Four Legislative Changes

One can see from the debates on surveillance legislation opinions are polarised between ardent supporters of the need for extensive powers required to protect national security and supporters of the protection for privacy and data protection are equally as strident in their views. The trigger for these four pieces of legislation being introduced is the state feeling the need to respond to events. In France the three terrorist attacks carried out in January 2015 was the accelerant to the new French surveillance laws being introduced so quickly.[60] For Canada it was the attacks at the Parliament buildings in October 2014.[61] It has not been one single event that resulted in the UK Government feeling the requirement to introduce new surveillance legislation. It has been a combination of events emanating from the terrorist attack by on Fusilier Lee Rigby in May 2013, the inability of the Conservative Party members of the 2010-2015 Coalition Government to pass the 2012 Communications Data Bill, the findings of the UK's ISC's reports on the killing of Lee Rigby[62] and on Privacy and Security,[63] and, the radicalising processes and threat groups like Islamic State pose to the security of the UK. The threat Islamic State and other Islamist groups pose to the security of the US can also be seen as the US passed the Freedom Act, but another factor has been the condemnation of NSA practices at national and international level. What is common between the four nations is the requirement that something has to be done to monitor a wide variety of communications in order to combat the terrorist threat in order to protect the right to life of their citizens.

Another similar issue raised in the introduction of the four pieces of legislation is that the surveillance powers are seen as overly intrusive and having minimal consideration for the

[60] Chrisafis [n. 51], Woods [n.53]
[61] Barber [n. 61]
[62] Intelligence and Security Committee of Parliament (2014) 'Report on the intelligence relating to the murder of Fusilier Lee Rigby' London: HMSO and ISC
[63] [n.39]

rights to individual privacy and data protection. Concerns range from wider surveillance powers not being acceptable under any circumstances where it intrudes into privacy and affects data protection, to more modest requests that surveillance practices need to be reined in. It is unfortunate this debate results in two polarised viewpoints of protecting the interests of national security and protecting individual rights that appears to lead to an impasse. One sticking point with those advocating the libertarian position is the dearth of evidence that bulk data collection of electronic communications has prevented terrorist attacks from happening.[64] This has also been the view of members of the judiciary. In *Klayman v Obama and others* Justice Leon was not convinced the NSA's bulk data collection actually stopped an imminent terrorist attack. He saw it as the most indiscriminate and arbitrary invasion of privacy adding, 'I am not convinced … the NSA's database has ever truly served the purpose of rapidly identifying terrorists in time-sensitive investigations.'[65] The findings in opinion polls asking citizens if state agencies should be allowed to carry out wider surveillance on electronic communications data are varied. A poll taken in late April 2015 revealed ordinary Canadians were increasingly expressing opposition to the Anti-terrorism Act[66] whereas a poll in France found that nearly two thirds of French citizens were in favour of restricting civil liberties to combat terrorism.[67]

As the International Commission of Jurists point out, the interests for national security and rights to privacy and data protection are not opposing poles, but a seamless web of protection incumbent upon the state.[68] As the Oklahoma Senator, James Lankford said during the Congress debate during the passage of the Freedom Act 2015 said:

[64] BBC News (2015) 'Emergency surveillance law faces legal challenge by MPs' 4th June 2015 retrieved from http://www.bbc.co.uk/news/uk-politics-33000160 [accessed 5th June 2015]
[65] (2013) Civil Action Number 13-0881 (RJL), at paragraph 66
[66] Barber [n.61]
[67] Kern [n.50]
[68] International Commission of Jurists, (2009) Assessing Damage, Urging Action Geneva: ICR, p.21

> 'National security and privacy are not mutually exclusive. They can be accomplished through responsible intelligence gathering and careful respect for the freedoms of [the law abiding].'[69]

Especially in relation to the UK and France, there is an opportunity for the European Union to take a lead, not just in the debate on where the balance should lay between the interests of national security and individual rights, but in introducing legislation such as a Directive giving wider surveillance powers related to electronic communications data as privacy rights and data protection is deeply imbedded into its legal framework. It is the latter points that give the EU the ability to appease both the supporters of protecting national security and those protecting privacy and breach the current impasse.

European Union Rights to Privacy and Data Protection

Digital Rights Case and EU Directive 2006/24/EC on Data Retention

An important decision by the European Court of Justice (ECJ) on data retention and privacy protection was given in *Digital Rights Ireland Ltd v Minister for Communications and others*.[70] 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. The ECJ found the 2006 and the 2002 Directives were invalid in relation to the data retention processed in connection with the provision of electronic communications data. Key to this decision was article 4 of the 2006 Directive that allowed Member States to adopt measures ensuring that data retained is

[69] Jennifer Steinhauer and Jonathan Weisman (2015) 'US Surveillance in Place Since 9/11 is Sharply Limited' The New York Times 2nd June 2015 retrieved from http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?_r=1 [accessed 3rd June 2015]

[70] Joined Cases C-293/12 (Digital Rights) and C-594/12 (Karntner Landesregierung)

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'[71]

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.[72]

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; the only conditions for Member States to retain data specified in article 4 was when it was necessary and proportionate to do so.[73] Examining the provisions of article 7 of the 2006 Directive, the ECJ said it should be read in conjunction with article 4. The problem in the wording of the Directive for the ECJ was its provisions did not ensure Member States had in place a particularly high level of protection nor did it ensure there was an irreversible destruction of the data at the end of the data retention period.[74] The ECJ did recognise the importance of data retention in relation to investigations into serious crime and terrorism saying:

[71] Article 4 EU Directive 2006/24
[72] *Digital Rights* Case C-293/12, paragraph 54
[73] D*igital Rights* Case C-293/12, paragraph 61
[74] *Digital Rights* Case C-293/12, paragraph 67

> '…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'[75]

In saying this, the ECJ held the problem with the 2006 Directive's data retention measures was in being too vague to justify its 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. Justification requires a legitimate aim and terrorism is certainly a legitimate aim and one that meets the objectives of general interest recognised by the EU. This includes the need to protect the rights and freedoms of others, including the important right, the right to life. As Ojanen states in his analysis of the Digital Rights Case, the more 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 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'[76]

The ECJ decision in Digital Rights is not a 'total knockout' to mandatory retention.[77] In drawing up legislation that specifically gives the legitimate aim for the retention such as to support investigations into acts of terrorism or serious organised crime, such as human trafficking, specifying realistic periods of data retention and sufficient safeguards into protecting rights of privacy and data protection would be sufficient.

EU Data Protection and Privacy Laws

EU law is clear that personal data is to be protected. Article 16 of the Treaty on the Functioning of the EU (TFEU) states that everyone has the right to the protection of personal data concerning them[78] and the European Parliament and the Council must act in accordance

[75] *Digital Rights* Case C-298/12, paragraph 51
[76] 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
[77] Ibid, p. 539
[78] TFEU C326/55 Article 16(1

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[79] as does article 39 in the Treaty of Union. The Charter of Fundamental Rights of the EU also is clear that everyone has the right to the protection of personal data concerning them.[80] 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'* [81] [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 EU[82] 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

Although it was being considered before the Snowden revelations, the EU is introducing changes to take effect by 2016 at the latest to 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);[83]
- 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.[84]

[79] TFEU article 16(2)
[80] 2000/C 364/01 Article 8(1)) 8(2)
[81] 2000/C 364/01 Article 8(2)
[82] 2000/C 364/01 Article 7
[83] 2012/0011 COD

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). In addition to the *Digital Rights Case*, another ECJ judgement underpinning EU law is the Court's decision in *Google Spain SL, Google Inc. v Agencia Espanola de Prrteccion de Datos (APED)*[85], which held that data retention without any link to risk or suspicion is not proportionate.

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

In order to replace the 2006 Data Retention Directive[86] following the *Digital Rights* decision, an example of an EU Member State taking a unilateral response is the UK with the Data Retention and Investigatory Powers Act 2014 (DRIPA). DRIPA allows for retention notices to be issued to ISP and CSP's to retain electronic communications data where it is necessary and proportionate when:

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.[87]

---

[84] 2012/0010 COD
[85] (2014) Case C-131/12
[86] Data Retention and Investigatory Powers Act 2014 Explanatory notes, paragraph 3
[87] S.1(1) Data Retention and investigatory Powers Act 204 and section 22(2) Regulation of Investigatory Powers Act 2000

This will require a communications operator to retain all the data specified in the notice,[88] up to a period not exceeding 12 months.[89] DRIPA also allows for interception warrants to be authorised when necessary the interests of national security.[90]

One problem with states adopting a unilateral response is the law in one state in not necessarily applicable to a communication company located in another state. Acknowledging this issue poses for DRIPA purposes, the UK appointed Sir Nigel Shienwald as special envoy on intelligence and law enforcement data sharing to lead discussions with international partners and ISP and CSP's 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 political frameworks or remedies for better arrangements for direct requests form UK agencies to companies that hold the data.[91]

Even though DRIPA has a sunset clause for it to expire 2016, in June 2015 two UK Members of Parliament have brought a legal challenge to the UK's High Court claiming DRIPA contains insufficient safeguards and as such it makes it incompatible with human rights.[92]

As one nation state attempts to apply a tough legal approach to transnational companies, it may not encourage compliance. It could be the opposite resulting in protracted legal battles affecting the state both financially and politically. This why the

[88] S.1(2) Data Retention and Investigatory Powers Act 2014
[89] S1(5) Data retention and Investigatory Powers Act 2014
[90] S.3(2) Data Retention and Investigatory Powers Act 2014
[91] 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]
[92] [n.64]

EU is not only best placed to take a lead, but is ethically best positioned to negotiate alongside third countries with ISP and CSP's. Such an approach is more likely to result in co-operation than forcing compliance in manually reading communications suspected to be related to terrorism.

Lee Rigby's Murder: An example Internet and Communications Service Providers Lack of Disclosure in Suspected Terrorism Related Communication

The UK's ISC report on the murder of Fusilier Lee Rigby by Michael outside Woolwich Barracks, London in May 2013 revealed his killers, Adebolajo and Adebowale, electronic communication with AQAP was not picked up by the UK's national security or counter-terrorism police officers.[93] In late 2012 one piece of communication via Facebook between Adebowale and AQAP operative referred to as FOXTROT, who was not known at the time to UK intelligence or counter-terrorism policing agencies, was not acted on at the time. In the communications with FOXTROT Adebowale expressed in a graphic and emotive manner his desire to murder a British soldier. FOXTROT encouraged Adebowale and suggested several methods of how he could successfully carry out the attack.

The company on whose system this online exchange took place closed some of Adebowale's accounts before the murder of Lee Rigby was carried out. The ISC learnt that internet and communications service providers use various automated techniques for identifying accounts the provider believes are breaking the terms of service such as those linked to child exploitation and to illegal acts such as inciting violence.[94] GCHQ reported to the ISC they only instigate actions when they receive a tip off or a complaint from another user or a provider. Unlike child exploitation cases where ISP

[93] Intelligence and Security Committee of Parliament (2014) 'Report on the intelligence relating tot eh murder of Fusilier Lee Rigby' London: HMSO, pp.119-136
[94] Ibid p.128

and CSP's regularly pass on information to the appropriate authorities, GCHQ added that for accounts linked to terrorism, information is rarely passed to the authorities.[95]

Even though Adebowale's eleven social media accounts were linked to terrorist activity, while the accounts were disabled via an automated process, communications providers do not manually review the content of the accounts nor pass on any information to the relevant authorities. Regarding this practice by communications providers, 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, had 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'.[96]

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. The current policy adopted by ISP and CSP's led to the GCHQ Director saying:

> 'However much [technology companies] may dislike it, they have become the command-and-control networks of choice for terrorists and criminals'.[97]

This situation is not unique to the UK this is an international problem requiring an international response for which the EU is well placed to take a lead. If this is not

[95] Ibid p.128
[96] Ibid p.129
[97]

done Member States will take unilateral decisions or bi-lateral agreements regarding the requirement that ISP and CSP's co-operate to supply of information suspected to be terrorist related. As many ISP and CSP's are based outside many Member States, even the EU itself, they are not obliged to retain and provide communications data to relevant authorities. As the EU represents 28 Member States it has the potential leverage to encourage third countries such as the US, Canada, and states the EU have EU Neighbourhood Polices agreement to work in co-operation with communications providers under a uniform legislative policy. *Prima facie* this may appear an idealistic and naïve. With the current international pressure regarding the concerns for national security and protecting the right to life of citizens, negotiations with ISP and CSP's regarding the forwarding of communications data to relevant authorities is more likely to obtain co-operation by an approach from the EU. As customer privacy and data protection is sacrosanct to ISP and CSP's, the position the EU holds regarding these legal issues makes it more likely that ISP and CSP's will listen to the EU. By looking for co-operation rather than compulsory data supply without clear and enshrined data protection will help ensure the needs of national security and data protection is equitably balanced.

Conclusion

The debate over the calls for wider surveillance powers to protect the interests of national security and the objection to such powers on the grounds of citizens' right to privacy and data protection will always be a constant in society. There are merits in both sides of the debate. It would be disingenuous to dismiss completely the rationale of governments and their intelligence and policing agencies claims that as electronic communication methods advance so must legislative powers in order to keep up with those advances. The reason behind this is that we all want to go about our daily lives in

safety without the fear of indiscriminate terrorist attacks. Likewise the requirement for sufficient safeguards in protecting rights to privacy and data protection should not be dismissed. As stated above, these are not opposing poles. The two positions should be intertwined as both areas of law are of equal importance, both are concerned with safety. One is related to citizens' personal safety and their right to life, the other being citizens use of electronic communications with the safety of there being no undue interference from the state. As rights to privacy and data protection is deeply embedded into its law is why the EU is the best placed body to take the lead in dealing with ISP and CSP's regarding co-operation, as these providers will feel their obligation to their customers' privacy is protected under the rule of law. In addition to this having a legislative framework that is common to twenty-eight Member States, the EU is more likely to ensure there are comparable legal provisions with third countries and this will help with intelligence exchange processes, all carried out with the reassurance privacy is protected, but more importantly so are citizens lives.