

# **Why in Widening Surveillance Powers of Electronic Communications, Co-Operation is needed with Internet and Communications Service Providers**

**David Lowe**

Liverpool John Moores University

Law School

Redmonds Building

Brownlow Hill

Liverpool L3 5UG

UK

Email: [D.Lowe@ljmu.ac.uk](mailto:D.Lowe@ljmu.ac.uk)

Tel No: 0151 231 3918

# **Why in Widening Surveillance Powers of Electronic Communications, Co-Operation is needed with Internet and Communications Service Providers**

## **Introduction**

There is no denying that the current international terrorist threat faced by many states around the world is real. The actions witnessed just in 2015 provides sufficient evidence of that as seen from the terrorist attacks in Paris in January 2015, to attacks seen in June 2015 in Kuwait, Tunisia and France and of late in Turkey and again in France in August 2015 where an attack was prevented by the courage of travellers on a train travelling from Holland to France. One common thread through these attacks are that the terrorists are known to be in various states' intelligence systems and yet their intended actions were not picked up by intelligence analysts. One of the reasons for this has been the widespread and sophisticated use of electronic communications systems by terrorist groups, especially the group Islamic State (also referred to as ISIL or Daesh). Another problem facing security and counter-terrorism policing agencies is in gaining access to communications data held by Internet Service Providers (ISP) and Communications Service Providers (CSP). By examining the current terrorist threat facing many states and terrorist groups' use of electronic communications, as well as the concerns over the surveillance society, this article looks at the proposed and recently passed legislation regarding surveillance of electronic communications in a number of states. One key issue why some of the legislative provisions will fail to achieve its intended outcome will be in the failure to secure the co-operation of ISP and CSP's. This article proposes that as privacy rights and data protection is deeply embedded within its law, the European Union (EU) has the opportunity to become a major international actor on the world stage in seeking that co-operation with ISP and CSP's in securing access to communications data and its retention.

## **The Current Terrorist Threat**

The civil war in Syria, conflicts in Libya since the fall of Colonel Gaddafi<sup>1</sup> and the control of large parts of Iraq by the group Islamic State has allowed a vacuum to exist enabling Islamist groups, in particular Islamic State and the Al Qaeda affiliate, Jabhat al-Nusra Front in Syria and Libya's Dawn Militia to flourish and become more powerful in these conflict zones.

These groups do not just pose a threat to the security of the conflict zones, they pose a threat to the security of nations around the world. This threat is enhanced by these terrorist groups' skilful use of electronic communications, in particular social media, in radicalising citizens and influencing them either to join these groups in the conflict zones or carry out terrorist attacks in their home state.

In January 2015 the head of the UK's intelligence agency MI5, Andrew Parker, pointed out that in monitoring the sophisticated use of electronic communications by terrorist groups under current legal conditions, it is virtually impossible to prevent every type of attack.<sup>2</sup> The alarming increase in the number of citizens who have travelled to Syria and Iraq to fight with Islamic State has led to the Director of the EU's policing agency Europol, Rob Wainwright, to warn of the security gap facing EU policing agencies as they try to monitor online communications of terrorist suspects. He says this is compounded by the fact that by being in Syria and Iraq these suspects are effectively out of reach.<sup>3</sup> On the difficulties the security and policing agencies are currently facing, 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.<sup>4</sup> Berger and Morgan

claim the number of Islamic State Twitter accounts could be as high as 90,000<sup>5</sup> thereby nearly doubling the number of daily tweets from Islamic State.

Katz highlights the difficulty intelligence and policing agencies face in monitoring social media and encrypted electronic communications, where again just using the example of Twitter, she reports how Islamic State is circumventing the blocking of their social media accounts.<sup>6</sup> One method being Islamic State account holders possess multiple back-up accounts and tweet followers to follow and retweet up to six accounts at a time. For Katz the threat of Islamic State on Twitter is real. She says Twitter alone is a launch pad for Islamic State recruitment or calls for lone wolf attacks or to send dangerous messages into every corner of the world. Twitter is not the only social media method of electronic communication used, groups like Islamic State also use other forms of social media and electronic communication to get their messages out to the wider world. Using the Twitter example helps to explain why it is important that intelligence and policing agencies co-ordinate their efforts in monitoring terrorist groups use of electronic communications and why they need wider powers of surveillance of electronic communications.

### **Concerns over the Surveillance Society: The Snowden Revelations**

Granting intelligence and policing agencies wider surveillance powers generates fears of a surveillance society where data protection and rights to privacy are abused by those agencies. In 2013 those fears were confirmed following the revelations by the former employee of the US' National Security Agency (NSA), Edward Snowden on the practices of the NSA and the UK's GCHQ in relation to Operation PRISM.<sup>7</sup> 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.<sup>8</sup> Snowden 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 saying 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’.<sup>9</sup> 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 Snowden passed on regarding the NSA’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.<sup>10</sup> This followed on from earlier reports that GCHQ accessed the NSA’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.<sup>11</sup>

The shock waves of the NSA’s actions reverberated around the world, more so when it was revealed that politicians in the EU Member States were also spied on by the NSA, in particular the German Chancellor Angela Merkel.<sup>12</sup> During this revelation the difference in legal culture between the EU and the US raised its head regarding individual’s rights 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.<sup>13</sup>

### **Western States’ Legislative response: Widening surveillance powers on electronica communications**

The summer of 2015 saw radical changes in some states’ legislation governing surveillance of electronic communications. In May 2015 the French National Assembly adopted a Bill on intelligence gathering that came into effect at the end of July 2015. This

legislation allows French authorities to vacuum up bulk communications data so it can be subject of analysis for ‘potentially suspicious behaviour’, place cameras in private houses and install key-logger devices that record every key stroke on a targeted computer in real time. Another provision within the Act is regarding ISP and CSP’s to install complex algorithms that flag up suspect behaviour patterns online such as key words used, site visits and contacts made. Also in May 2015 the Canadian government passed the Anti-Terrorism Act 2015. Among the Act’s key provisions is an amendment to code 83.233 of the Canadian Criminal Code that allows state authorities to monitor computer data where the material amounts to terrorist propaganda. Other provisions include widening information of air passenger lists and allowing for wider information sharing to ‘protect Canada against activities that undermines the security of Canada’.

In June 2015 the US Congress passed the Freedom Act 2015 that amends the Foreign Intelligence Surveillance Act 1978 (FISA). Congress allowed the 2001 Patriot Act provisions, passed shortly after the 9/11 attack on the US by Al Qaeda, to expire under its sunset clause. It was the Patriot Act amendments to FISA that caused the greatest consternation regarding abuse of rights to privacy and data protection by federal agencies. In addition to the outcry from liberty organisations following the Snowden revelations, influential in the Freedom Act being adopted was in following the direction by given in decisions by the US courts. In 2015 the case *American Civil Liberties Union (ACLU) and others v Clapper and others*<sup>14</sup> 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*<sup>15</sup> 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, this was illegal, depriving the applicants of their constitutional rights.<sup>16</sup> At the time of making their decision the Court did recognise that section 215 FISA was scheduled to expire and that Congress were to debate the Patriot Act's sunset clause.<sup>17</sup> 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 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.'<sup>18</sup>

As a result of the Freedom Act's amendments US federal agencies will only be permitted to gather bulk communications data where it is targeted to 'specific section term'. A specific section term is defined as that which, '...specifically identifies a person, account, address, or personal device or any other specific identifier.'<sup>19</sup> The Act makes it clear a specific identifier does not include an identifier that has no limit to the scope of information sought and, unless the provider is subject of an authorised investigation for which the specific selection term is used as the basis for the use, it cannot be a method of surveillance gathering.

Regarding unlawfully obtained information a court can order a correction of a deficiency. 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.<sup>20</sup> 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,<sup>21</sup> but where necessary they can be released in a redacted form.<sup>22</sup>

In the autumn of 2015 the UK government will be introducing an Investigatory Powers Bill. The UK government has stated the importance in the requirement of such legislation being introduced as they see it being necessary in:

1. Addressing ongoing capability gaps that are severely degrading the ability of law enforcement and intelligence agencies ability to combat terrorism and other serious crime;
2. Maintaining the ability of UK intelligence agencies and law enforcement to target the online communications of terrorists, paedophiles and other serious criminals;
3. Modernising the UK's law in the areas of terrorism and serious crime and ensure it is fit for purpose;
4. Providing for appropriate oversight and safeguard arrangements.<sup>23</sup>

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.

### **Similarities in Issues Between the Four Legislative Changes**

Regarding 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. The trigger for these four pieces of legislation being introduced is the state feeling the need to respond to events. In France the Paris attacks in January 2015 was the accelerant to the new French surveillance laws being rapidly introduced.<sup>24</sup> For Canada it was the attacks at its Parliament buildings in October 2014.<sup>25</sup> At the time it was announced, it has not been one single event that resulted in the UK Government feeling the need to introduce new surveillance legislation. It was 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 Parliamentary Intelligence and Security Committee's (ISC) reports on the killing of Lee Rigby<sup>26</sup> and on Privacy and Security,<sup>27</sup> and, the radicalising processes and threat groups like

Islamic State pose to the security of the UK. However the killing of 30 UK citizens in Tunisia in June 2015 has added fuel to the clamour for wider surveillance powers on electronic communications. While the constant threat Islamist groups pose to the security of the US is behind the Freedom Act 2015, what differentiates the US changes to its surveillance laws from the other three states emanates from the condemnation of NSA practices at national and international level. What is common between the four nations is in order to protect the right to life of their citizens is the requirement something has to be done to monitor a wide variety of communications in order to combat the terrorist threat.

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 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. Regarding the French law, the main criticism is the lack of scrutiny of authorities' surveillance practise by the judiciary. French liberty organisations have argued this move does not fit in a true democracy where state agencies should be governed by the rule of law adding that true impartiality can only be through the judiciary, as judges are suitably placed to decide if there should be restrictions of fundamental freedoms.<sup>28</sup> The concerns expressed regarding the Canadian Anti-Terrorism Act is encapsulated in the criticism from Canada's Privacy Commissioner, 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.'<sup>29</sup>

Regarding the US' Freedom Act Neemah Guiliani, the ACLU's legislative counsel, acknowledged the Act as a historic step forward, but is not as strong as the ACLU wanted it

to be. She added the ACLU would like to see US citizens 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, and, Congress reject efforts to expand surveillance through cybersecurity information-sharing legislation.<sup>30</sup> Even though the details of the UK's Investigatory Powers Bill have yet to be released, the UK government's rhetoric in relation to the Bill has not escaped criticism regarding the impact the proposed powers will have on privacy rights 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'<sup>31</sup>

It is unfortunate this debate results in two such polarised viewpoints regarding protecting the interests of national security and protecting individual rights, as this leads 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.<sup>32</sup> 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.'<sup>33</sup> 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<sup>34</sup> whereas a poll in France found that nearly two thirds of French citizens were in favour of restricting civil liberties to combat terrorism.<sup>35</sup>

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.<sup>36</sup> As the Oklahoma Senator, James Lankford said in Congress during the passage of the Freedom Act 2015:

‘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].’<sup>37</sup>

Especially in relation to the UK and France, there is an opportunity for the EU to take a positive lead in the debate on where the balance should lay between the interests of national security and individual rights. As privacy rights and data protection is deeply imbedded into its legal framework, with the third countries such as the US and Canada it has international treaties with, it can approach ISP and CSP’s regarding communications data retention and the granting of access to intelligence and policing agencies under an authorisation. As such it would give the EU the ability to appease the supporters of protecting national security and those protecting privacy thereby breaching the current impasse.

### **Co-operation with ISP and CSP’s: The EU’s opportunity to take the Lead**

As privacy and data protection laws are not only deeply embedded in EU law but are taken seriously by the EU, now is the opportunity for the EU to become a major international actor on the political scene in securing co-operation with ISP and CSP’s in granting access to and retaining their communications data. Privacy rights and personal data are protected under article 16 of the Treaty of on the Functioning of the EU, the Treaty of Union and the Charter of Fundamental Rights of the EU. All three of these legal documents are clear that EU bodies and its member states can only process personal data fairly for specified purposes on the basis of consent of the person concerned or on some other legitimate basis laid down by law. To see how the EU take these provisions seriously and how its institutions are not deterred in over-turning legislative provisions related to privacy rights and data protection one only has

to look at the important decision by the European Court of Justice (ECJ) in *Digital Rights Ireland Ltd v Minister for Communications and others*.<sup>38</sup> The case centred mainly on Directive 2006/24/EC that laid 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 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 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 in 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' Article 4 EU Directive 2006/24

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.<sup>39</sup>

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.<sup>40</sup> 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.<sup>41</sup> 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’<sup>42</sup>

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 proportionality cannot be justified in imposing limitations on citizens’ rights. Justification requires a legitimate aim and terrorism is certainly a legitimate aim being 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’<sup>43</sup>

The ECJ decision in Digital Rights is not a ‘total knockout’ to mandatory retention.<sup>44</sup> 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. 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 Proteccion de Datos (APED)*<sup>45</sup>, which held that data retention without any link to risk or suspicion is not proportionate.

Seeking co-operation with ISP and CSP's requires a unified international response. There is little one nation state can do on its own, such as the UK has done with the Data Retention and Investigatory Powers Act 2014 that was introduced in response to the Digital Rights Case. This Act requires communications operators to retain data<sup>46</sup> up to a period not exceeding 12 months.<sup>47</sup> It also allows for interception warrants to be authorised to UK intelligence and policing agencies to access the communications data when necessary the interests of national security.<sup>48</sup> One problem with states adopting a unilateral response is the law in one state is not necessarily applicable to communications companies located in another state. Where this situation exists there is no obligation on ISP and CSP's to comply with any requests or authorisations. When one nation state attempts to apply a tough legal approach on transnational companies, it may not encourage compliance. It is more likely to result in protracted legal battles affecting the state both financially and politically. This why the 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 from the providers rather than forcing compliance in manually reading communications suspected to be related to terrorism.

An example of how co-operation with ISP and CSP's can assist in counter-terrorism investigations is seen in the UK's ISC report on the murder of Fusilier Lee Rigby outside Woolwich Barracks, London in May 2013.<sup>49</sup> It revealed that in late 2012 one of his killers, Adebowale communicated via Facebook with an AQAP operative referred to as FOXTROT. FOXTROT was not known at the time to UK intelligence or counter-terrorism policing agencies and so was not acted upon at the time. In these

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 ISP and CSP's 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<sup>50</sup> 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 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.<sup>51</sup>

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'.<sup>52</sup>

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 that review finds information of a specific intention to commit a terrorist act is present, to pass it 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'.<sup>53</sup>

This situation is not unique to the UK, this is an international problem requiring an international response, hence why it is suggested the EU is well placed to take a lead. *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. It is time to change the intelligence paradigm from 'need to know' to 'need to share'.

## **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 using electronic communications in 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. Reassurance there will be no unnecessary use or abuse of data protection and rights to privacy is more likely to result in these providers feeling their obligation to their customers' privacy is protected under the rule of law. The current terrorists' use of electronic communications is enhancing the international threat nation states are facing resulting in calls for wider surveillance powers to counter the threat. For this to be successful effective co-operation is required from ISP and CSP's, many of whom are supranational companies, as we have now moved to a communications age requiring a 'need to share' intelligence model.

---

<sup>1</sup> BBC News (2015) 'Libya Trial' 28<sup>th</sup> July 2015 retrieved from <http://www.bbc.co.uk/news/world-africa-33688391> [accessed 28th July 2015]

<sup>2</sup> 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]

- 
- <sup>3</sup> BBC News (2015) 'Terror threat posed by thousands of EU nationals' 13th January 2015 retrieved from <http://www.bbc.co.uk/news/uk-30799637> [accessed 22nd January]
- <sup>4</sup> 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]
- <sup>5</sup> Berger JM and Morgan J (2015) 'The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter' Center for Middle East Policy at Brookings, 20th March 2015 retrieved from [http://webcache.googleusercontent.com/search?q=cache:nUpiATbv50wJ:www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis\\_twitter\\_census\\_berger\\_morgan.pdf+&cd=1&hl=en&ct=clnk&gl=uk](http://webcache.googleusercontent.com/search?q=cache:nUpiATbv50wJ:www.brookings.edu/~media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf+&cd=1&hl=en&ct=clnk&gl=uk) [accessed 19th June 2015]
- <sup>6</sup> Katz R (2015) 'How Islamic State is still Thriving on Twitter' InSite Blog on Terrorism & Extremism 11th April 2015 retrieved from <http://news.siteintelgroup.com/blog/index.php/entry/377-how-the-islamic-state-is-still-thriving-on-twitter> [accessed 18th June 2015]
- <sup>7</sup> Greenwald, Glenn (2014) *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State* New York: Metropolitan Books, pp.33-42
- <sup>8</sup> 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]
- <sup>9</sup> 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]
- <sup>10</sup> MacAskill, 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]
- <sup>11</sup> Nick Hopkins (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]
- <sup>12</sup> Ibid p.141
- <sup>13</sup> Cian Murphy (2012) *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* Oxford: Hart Publishing, p.149
- <sup>14</sup> (2015) Case 14-42
- <sup>15</sup> (2013) Civil Action Number 13-0881 (RJL)
- <sup>16</sup> Ibid p.94
- <sup>17</sup> Ibid p.96
- <sup>18</sup> Ibid pp.96-97
- <sup>19</sup> s.201(b) Freedom Act 2015
- <sup>20</sup> s.301 Freedom Act 2015
- <sup>21</sup> s. 602(a) Freedom Act 2015
- <sup>22</sup> s. 602(b) Freedom Act 2015
- <sup>23</sup> 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]
- <sup>24</sup> 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], Mike Woods (2010) '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]
- <sup>25</sup> 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]
- <sup>26</sup> Intelligence and Security Committee of Parliament (2014) *Report on the intelligence relating to the murder of Fusilier Lee Rigby* London: HMSO and ISC
- <sup>27</sup> Intelligence and Security Committee of Parliament (see note 25 above)
- <sup>28</sup> Mike Woods (see note 24 above)
- <sup>29</sup> Ibid

- 
- <sup>30</sup> 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]
- <sup>31</sup> Jim Killock (2015) Open Rights Group Supporters Newsletter June 2015 retrieved from <https://www.openrightsgroup.org/support-org> [accessed 23rd June 2015]
- <sup>32</sup> 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]
- <sup>33</sup> (2013) Civil Action Number 13-0881 (RJL), at paragraph 66
- <sup>34</sup> Barber (see note 45 above)
- <sup>35</sup> Kern (see note 34 above)
- <sup>36</sup> International Commission of Jurists, (2009) *Assessing Damage, Urging Action* Geneva: ICR, p.21
- <sup>37</sup> 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](http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html?_r=1) [accessed 3rd June 2015]
- <sup>38</sup> Joined Cases C-293/12 (Digital Rights) and C-594/12 (Karntner Landesregierung)
- <sup>39</sup> Digital Rights Case C-293/12, paragraph 54
- <sup>40</sup> Digital Rights Case C-293/12, paragraph 61
- <sup>41</sup> Digital Rights Case C-293/12, paragraph 67
- <sup>42</sup> Digital Rights Case C-298/12, paragraph 51
- <sup>43</sup> 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
- <sup>44</sup> *Ibid*, p. 539
- <sup>45</sup> (2014) Case C-131/12
- <sup>46</sup> S.1(2) Data Retention and Investigatory Powers Act 2014
- <sup>47</sup> S1(5) Data retention and Investigatory Powers Act 2014
- <sup>48</sup> S.3(2) Data Retention and Investigatory Powers Act 2014
- <sup>49</sup> Intelligence and Security Committee of Parliament (see note 66 above), pp.119-136
- <sup>50</sup> *Ibid* p.128
- <sup>51</sup> *Ibid* p.128
- <sup>52</sup> *Ibid*, p.129
- <sup>53</sup> *Ibid* p.129