UCLAN

WORKSHOP ON TRANSNATIONAL SECURITY AND HUMAN RIGHTS

Time to plug the UK security gap: why there is a need to widen surveillance on electronic communications data

Dr David Lowe
Liverpool John Moores University

Email: D.Lowe@ljmu.ac.uk

Tel No: 0151 231 3918

Time to plug the UK security gap: why there is a need to widen surveillance on electronic communications data

Introduction

This paper examines whether there is a need for the UK to introduce legislation regarding further surveillance powers for the intelligence and policing agencies to conduct surveillance on electronic communications data. Both legally and politically t is a controversial issue. One side of the debate argues the need for such powers in order to assist the intelligence and policing agencies in their investigations, especially in relation to preventing acts of terrorism occurring to keep citizens safe from such attacks. The other side of the debate raises serious concerns of rights to privacy and data protection with the main issue being on the lack of sufficient safeguards against abuses by the agencies in their acquisition and retention of communications data.

By looking at the current terrorist threat facing the EU (which includes the UK) focusing mainly on the threat the terrorist group Islamic State pose considerations are given to both sides of the debate. This includes an examination in how Islamic State use electronic communications, especially its social media sources by using the example of their use of Twitter and issues surrounding the difficulty policing agencies are having in monitoring this group's activities on communications sources. By having such agencies monitoring electronic communications use raises concerns over the surveillance society, a concern that was exacerbated by the former US National Security Agency (NSA), Edward Snowden's revelations in how, why and what the NSA was monitoring and its relationship with the UK's intelligence agency, General Communications Headquarters (GCHQ).

By looking at what communications is subject to the requests for wider surveillance this paper will examine the current legislative provisions authorising surveillance by the intelligence and policing agencies surveillance of electronic communications. This includes

an analysis of the findings of the European Union's court, the European Court of Justice's (ECJ) decision in the Digital Rights case where after deciding that the EU's legislative provisions on data protection were insufficient resulted in the UK introducing the Data Retention and Investigatory Powers Act 2014 that allows intelligence and policing agencies to request from communications providers electronic communications data related to their investigations. With the 2014 Act having a sunset clause expiring in December 2016 and taking into account recent Parliamentary reports, it is examined if there is a need for a new legislation in the UK that codifies al the current legislation governing the surveillance of electronic communications. This looks more likely as the Queen's Speech in May 2015 revealed an Investigatory Powers Bill will be introduced during the 2015/16 Parliament. The position submitted here is that new legislation is needed as wider powers are required to allow the intelligence and policing agencies the ability to monitor terrorist group's increasing sophisticated and wide use of electronic communications, provided there are sufficient safeguards related to data protection. Those safeguards can only be truly secured via judicial supervision in granting the respective authorities to the intelligence and policing agencies. Underpinning this submission is that due to the international nature of the terrorist threat facing national states and the use by terrorist groups of communications, we have moved to an era where intelligence in no longer on a 'need to know' basis to one where it is a 'need to share'. This includes obtaining the co-operation of internet and communications service providers.

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]

Country	Estimated number of citizens travelling to join Islamic State in Syria, September 2014	Estimated increase in number of citizens travelling to join Islamic State in Syria, January 2015	Total number of citizens travelling to join Islamic State in Syria
France	900	500	1,400
UK	400	200	600
Germany	320	280	600
Belgium	350	100	450

Table 1: Number of Citizens joining Islamic State in Syria (Sources: Mezzfiorie (2014), Murray (2014), Maminghano (2014), BBC News (2015a))

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. Recent examples of this include:

1. May 2014, Brussels, Belgium, four people killed at the Jewish Museum in Brussels by an Islamic State militant, Muhdi Nemmouche;[2]
2. January 2015, Paris, France, 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;[3]
3. January 2015, Paris, France, 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

[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]

[2] 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]

[3] 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]

Supermarket in Paris, killing four of the hostages before the French police stormed the building killing Coulibaly;[4]

4. January 2015, UK, Imran Khawaja was convicted and received a prison sentence at the Old Baily Court in London for preparing acts of terrorism after attending a terrorist training camp in Syria. Khawaja 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.[5]

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. Currently a number of issues and accusations have been raised with the three Dawood sisters and their nine children from Bradford, UK who travelled to Syria to live in the Islamic State caliphate.[6]

On Friday 26th June three terrorist attacks were carried out in France[7], Kuwait[8] and Tunisia[9] that have all been linked to Islamic State. Regarding the attack in Tunisia by Seifeddine Rezgui has resulted in the highest number of UK causalities since the Al Qaeda inspired attack in London on the 7th July 2005. It is reported that Razgui was inspired and supported by Islamic State to carry out the attack where he killed 37 tourists on a beach and in a hotel in Sousse, Tunisia with the death toll of UK citizens expected to be around 30. These attacks demonstrate the international nature of the current terrorist threat and why it requires an international co-operative response.

---

[4] 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]

[5] 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]

[6] BBC News 2015 'Bradford Dawood family "split to cross Syria border"' retrieved from http://www.bbc.co.uk/news/uk-33197308 [accessed 22nd June 2015]

[7] BBC News 2015 'Islamic state linked to France factory beheading' 30th June 2015 retrieved from http://www.bbc.co.uk/news/world-europe-33332862 [accessed 1st July 2015]

[8] BBC News 2015 'Kuwait Shia mosque attack: Bomber was Saudi' 28th June 2015 retrieved from http://www.bbc.co.uk/news/world-middle-east-33303795 [accessed 1st July 2015]

[9] BBC News 2015 'Tunisia attack: what we know about what happened' 30th June 2015 retrieved from http://www.bbc.co.uk/news/world-africa-33304897 [accessed 1st July 2015]

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 groups, it is virtually impossible to prevent every type of attack.[10] 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.[11] His concerns centre on the difficulties the security and 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.[12] Berger and Morgan claim the number of IS Twitter accounts could be as high as 90,000[13] thereby nearly doubling the number of daily tweets from IS. 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

[10] 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]

[11] 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]

[12] 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]

[13] 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 Brooking, 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 [accessed 19th June 2015]

reports how IS is circumventing the blocking of their social media accounts.[14] One method being IS account holders having multiple back-up accounts and tweet followers to follow and retweet up to six accounts at a time. For Katz the threat of IS on Twitter is real. She says Twitter alone is a launch pad for IS recruitment or calls for lone wolf attacks or to send dangerous messages into every corner of the world. This helps to explain why it is important that policing agencies co-ordinate their efforts in monitoring terrorist groups use of electronic communications.

The terrorist attacks carried out in 2015 have been mainly low-level attacks with the use of small arms. Being relatively easy to plan and execute, it demonstrates why it is important that agencies work together and have the capability to monitor electronic communications, especially where it requires the co-operation of the internet and communications service providers. In relation to communications linked to terrorist activity we have entered the era from 'need to know' to 'need to share'. This includes in the retention and sharing of electronic communications data form internet and communications service providers.

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 former NSA employee, Edward Snowdon on the practices of the NSA and GCHQ in relation to Operation PRISM.[15] 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

[14] 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]

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

Google, Microsoft, Facebook, Yahoo, Skype and Apple.[16] 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'.[17] 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.[18] This followed on from earlier reports that GCHQ accessed the FSA's Prism programme to secretly gather intelligence, where between May 2012 –April 2013, 197 Prism intelligence reports were passed onto the UK's security agencies, MI5, MI6 and Special Branch's Counter-Terrorism Unit.[19]

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.[20] As Greenwald (the *Guardian* newspaper

[16] 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]
[17] 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]
[18] 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]
[19] 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]
[20] Ibid p.141

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.'[21]

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.[22] 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.[23] 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.

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

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

the public interest.'[24] As a result, among its recommendations is that all the current legal frameworks on surveillance are replaced with a new Act of Parliament.[25] 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.[26]

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'.[27] 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.'[28]

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 director of policy of the Liberty saying, 'Yes …That is the price you pay to live in a free society.'[29] 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'.[30] For some this response may appear astounding and irresponsible while for others this stance is plausible.

---

[24] Intelligence and Security Committee of Parliament (2015) 'Privacy and Security: A modern and transparent legal framework' London: Her Majesty's Stationary Office, p/2
[25] Ibid p. 118
[26] Ibid pp.118-119
[27] 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
[28] Ibid, p.4 paragraph 5
[29] Intelligence and Security Committee of Parliament (see note 21) pp. 35-36
[30] Ibid p.36

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'.[31] 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. 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[32]

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

[31] Simon McKay (2015) 'Covert Policing: Law and Practice' (2nd edition) Oxford: Oxford university Press, p.129
[32] 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

surveillance on electronic communications data that stringent controls are in place protecting privacy and data protection.

Summary of UK Surveillance Powers on Electronic Communications Data

This section looks at the key pieces of UK legislation governing surveillance of electronic communications. From just these examples one can see why it is perceived the law governing surveillance of electronic communications data is complex and how it has been developed piecemeal. This was a point that led to the ISC stating that by being developed in a piecemeal way the law is unnecessarily complicated giving the ISC serious concerns regarding the lack of transparency, which they rightly claim is not in the public interest.[33]

Regulation of Investigatory Powers Act 2000 (RIPA)

The two RIPA authorities worth discussing are interception warrants and acquisition of data authorities, issued by the Secretary of State in relation to the surveillance of electronic communications data available to the intelligence and policing agencies in the UK. The main difference between the two authorities is an interception warrant is in relation to investigations where an individual is suspected to have involvement in acts of terrorism or serious criminal activity. An interception warrant allows the intelligence and policing agencies to monitor targeted individual's use of various forms of communication. An authority to acquire communications data is in essence an authority requiring Internet Service Provider (ISP) and Communications Service Provider's (CSP) to disclose communications data they hold intelligence and policing agencies believe would assist an investigation.

Interception Warrants

Part 1 of RIPA allows for the interception, acquisition and disclosure of communications data by state agencies authorised to do so. Section 5 RIPA allows the Secretary of State to issue an interception warrant to obtain information about the

[33] Intelligence and Security Committee (see note 21) p.2

communications a person is using both in the UK and in territory outside the UK.[34] An interception warrant can only be issued where it is proportionate to do so and necessary on the grounds of national security, or to prevent or detect serious crime or it is for the purpose of safeguarding the economic well-being of the UK.[35] An interception warrant can only be issued when the application is made by or on behalf of:

1. The Director-General of the Security Service (MI5);
2. The Chief of the Secret Intelligence Service (MI6);
3. The Director of GCHQ;
4. Director of the National Crime Agency;
5. The Commissioner of the Metropolitan Police, Northern Ireland Police Service and chief constables in the rest of Britain;
6. The Commissioner of HM Customs and Revenue;
7. The Chief of Defence Intelligence;
8. A person who for the purposes of any international mutual assistance agreement is the competent authority of a country or territory outside the UK.[36]

Important for the interception warrants is that it names either the person as the interception subject or the premises where the interception is to take place.[37] As circumstances can change during an investigation thereby altering the focus of that investigation, RIPA allows for the Secretary of State to modify the provision in the interception warrant.[38]

Regarding safeguards that are in place the Secretary of State must specify the number of persons to whom the data is disclosed or made available, the extent to which the data is disclosed or made available, and the extent to which the data is copied along with the number of copies made.[39] The communications data is to be destroyed as soon as there are no longer any grounds for retaining it[40] and where it is retained, it can only be done so on the grounds it

[34] s.4 RIPA
[35] s.5 RIPA
[36] s.6 RIPA
[37] s.8 RIPA
[38] s.10 RIPA
[39] s.15 (2) RIPA
[40] s.15(3) RIPA

is necessary in the interests of national security, to prevent or detect crime or disorder or for safeguarding ten economic well-being of the UK.[41]

Acquisition and Disclosure of Communications Data

Part I Chapter II RIPA allows the Secretary of State to authorise intelligence and policing agencies[42] to obtain communications data where, among the qualifications for the state to interfere with the right to privacy it is believed to be necessary in the interests of national security, or to prevent or detect crime, or it is in the interests of the economic well-being of the UK, or it is in the interests of public safety.[43] The authorisation notice must be in writing, describing the category of communications data the authority applies to.[44] Where the authority is for communications providers to disclose data in their possession[45] the authority must describe the communications data the provider has to obtain and disclose, specifying the reason why (that is on the grounds of it being necessary in the interests of national security or one of the reasons given in s. 22(2) RIPA) and specify the manner in which disclosure is to be made.[46] Where it is either no longer necessary or proportionate for the requirements of the notice to be complied with, the notice shall be cancelled.[47]

RIPA Safeguards: The Interception of Communications Commissioner and Tribunal

Under RIPA the UK Prime Minister has to appoint an Interception of Communications Commissioner[48] whose role is to give the Tribunal assistance in relation any investigation by the Tribunal[49] and to keep under review the exercise of any power the Secretary of State makes under RIPA.[50] A Commissioner must either hold or have held

[41] S.15(4)(a) RIPA
[42] s. 25(1) RIPA
[43] s.22(2) RIPA
[44] s.23(1) RIPA
[45] s.22(4) RIPA
[46] s.23(2) RIPA
[47] S.23(9) RIPA
[48] S. 57(1) RIPA
[49] s.57(3)(a) RIPA
[50] s.57(4) RIPA

judicial office.[51] The Tribunal's jurisdiction is granted under section 7 Human Rights Act 1998 to investigate complaints that a public body has not acted in a manner that is compatible with the European Convention on Human Rights (ECHR)[52] and to consider complaints made by persons who are aggrieved as to the conduct of those who have carried out surveillance authorities.[53] A person can only challenge conduct where the surveillance authority was issued the Secretary of State, not where an authority is granted by a judicial authority.[54]

A RIPA authorisation must be compatible with the provisions of the ECHR and we can see how article 8 (right to privacy and family life) ECHR is incorporated into the conditions for granting both the interception warrants and the authorities requiring disclosure of communications data. UK liberty groups such as Big Brother Watch do not see these safeguards as sufficient regarding data protection. In the group's 2014 report on the police use of RIPA they see the safeguards as inadequate and there should be more stringent safeguards, especially on 'non-suspects' communications data saying that under the current conditions:

> '…in our view a court would probably hold that the restrictions on retention, storage and reproduction of external contents data and communications data are insufficiently robust, and that the UK is therefore in violation of its article obligations'[55]

To date these RIPA sections have not been successfully challenged in the courts. This may due to the decision of the European Court of Human Rights in *Klass v Germany* who examined article 8 ECHR. While acknowledging that surveillance is a necessary evil in a democracy, held that when the state carries out covert surveillance its actions must be

[51] s.57(5) RIPA
[52] s.65(2)(a) RIPA
[53] s.64(2)(b) RIPA
[54] S.65(7) RIPA
[55] Big Brother Watch (2014) 'Briefing Note: Why Communications Data (Metadata) Matter' retrieved from http://webcache.googleusercontent.com/search?q=cache:_dnTKjWRKNEJ:www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf+&cd=1&hl=en&ct=clnk&gl=uk [accessed 30th April 2015]

proportionate.[56] It appears to be the fact the Commissioner scrutinising authority applications must hold or have held a judicial office that has to date satisfied the courts.

Intelligence Services Act 1994 (ISA)

This Act applies to the three UK intelligence services, the Secret Intelligence Service (commonly referred to as MI6), the Security Service (commonly referred to as MI5) and GCHQ. It is aimed at legislating for their main surveillance practices, in particular GCHQ's interference with the various forms of communication it monitors.[57] The ISA also allows for surveillance warrants to be authorised under s.5 by the respective Secretary of State for the respective agencies (Foreign Secretary for MI6 and the Home Secretary or MI5 and GCHQ) to interfere with property or wireless telegraphy where the action is proportionate. For the:

1. Secret Intelligence Service (MI6) it has to be in the interests of national security especially in relation to the defence and foreign policies of the UK Government, or is in the economic interests of the UK or is to support the prevention or detection of serious crime;
2. Security Service (MI5) it has to be when it is carrying out its functions under the Security Service Act 1989. Under the 1989 Act those functions are the protection of national security, in particular threats from espionage, terrorism, sabotage, activities of agents of foreign powers or activities intended to overthrow parliamentary democracy by political, industrial or violent means. Other functions include protecting ten economic interests of the UK and in supporting the actions of police forces and the National Crime Agency;[58]
3. GCHQ when it is carrying out a function in the interests of national security, especially with reference to the defence and foreign policies of the UK, or in protecting the economic interests of the UK or in support of the prevention or detection of crime.[59]

These three agencies can also utilise the power under sections 5 and 25 RIPA regarding intrusion warrants and authorities for data disclosure as well the above ISA warrant to conduct surveillance. One can see that there are slight differences in the grounds for requesting an authority under ISA compared to RIPA, as they include the function of the

[56] (1978) (Application number 5029/71) at paragraph 68
[57] s.3 ISA
[58] s1. Security Service Act 1989
[59] Functions of GCHQ from s.3(2) ISA

defence of the UK and with regard to MI5, one can see the wide area of activity covered under s.1 Security Services Act 1989 this agency can get interfere with.

Wireless Telegraphy Act 2006 (WTA)

Section 48 WTA allows a person under an authority granted by the Secretary of State and Commissioners of Revenue and Customs[60] a broad power to intercept wireless or other communication with intent to obtain information as to the content of that communication, the details of the sender or addressee of the message.[61] As seen with RIPA, an interception authority under the WTA must be necessary and includes among others one of the following grounds:

1. Where it is in the interests of national security;
2. For the purpose of preventing or detecting crime or disorder;
3. Where it is in the interests of the economic well-being of the UK;
4. Where it is in the interests of public safety;
5. For the purpose of protecting public health.[62]

The authority must be in writing[63] and the authority may be general or specific, given to such a person for a specified period with the authority being subject to restrictions and limitations.[64]

In relation to RIPA interception warrants there appears to be little operational distinction between that and the WTA interception authority, as Anderson notes, both authorities might be used to intercept the same communications.[65] The WTA authority is more likely to be used by the UK intelligence services than the police, who will be more inclined to use RIPA authorities.

[60] s. 48(5) WTA
[61] s. 48 (1) WTA
[62] s.49(4) WTA
[63] s.49(7) WTA
[64] s.49(8) WTA
[65] Anderson, D (2015) 'A Question of Trust: Report of the Investigatory Powers Review' London: HMSO, p.97

The *Digital Rights* Case and the UK Response

In April 2014 the European Court of Justice (ECJ) held in *Digital Rights*[66] the provisions related to data protection and privacy rights under the 2006 Data Retention Directive[67] were invalid because they lacked specificity and sufficiency. As a result the UK introduced the Data Retention and Investigatory Act 2014 (DRIPA).

Digital Rights Case

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 Member States' legal provisions regarding the protection of fundamental rights and freedoms especially in the processing of personal data in the electronic sector processing of personal data and the protection of privacy. In essence the ECJ found that both of the Directives were invalid in relation to data retention processed in connection with the provision of available electronic communications data. Key to this decision was article 4 of the 2006 Directive that states Member States shall adopt measures to ensure that data retained is provided only to the competent national authorities in specific cases in accordance with national law adding:

> 'The procedures to be followed and the conditions to be fulfilled ion order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member state in its national law, subject to the relevant provisions of EU law or public international law and in particular the [European Convention on Human Rights] as interpreted by the European Court of Human Rights'[68]

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

[66] Case C-293/12
[67] Data Retention and Investigatory Powers Act 2014 Explanatory notes, paragraph 3
[68] Article 4 EU Directive 2006/24

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.[69]

Looking at the inadequacies of article 4 in the 2006 Directive the ECJ held that article 4 did not expressly provide that access to the use of the data was strictly restricted for the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such crimes; all the conditions specified in article 4 as that Member States defined procedures to followed that were in accordance with necessity and proportionality requirements.[70] Examining the provisions of article 7 of the 2006 Directive regarding data protection and security that the ECJ said should be read in conjunction with article 4 held that it does not ensure a particularly high level of protection and security and the Directive as a whole did not ensure the irreversible destruction of the data at the end of the data retention period.[71] 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'[72]

In saying this, the ECJ decided the 2006 Directive's data retention measures were too vague to even justify these objectives as the rationale for the data retention. Simply stating retention should be carried out under the principles of necessity and be proportionality cannot be justified in imposing limitations on citizens' rights as the imposition of limitations requires a legitimate aim and terrorism is certainly a legitimate aim that is recognised as one that meets the objective s of general interest recognised by the EU and that includes corresponding with the need to protect the rights and freedoms of others, including the important right, the right

[69] *Digital Rights* Case C-293/12, paragraph 54
[70] D*igital Rights* Case C-293/12, paragraph 61
[71] *Digital Rights* Case C-293/12, paragraph 67
[72] *Digital Rights* Case C-298/12, paragraph 51

to life. In his analysis of the Digital Rights Case Ojanen states, 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'[73]

Ojanen recognised, the ECJ decision in Digital Rights is not a 'total knockout' to mandatory retention.[74] The EU requires form its Member states when drawing up legislation to specify the legitimate aim for the retention. Examples of specificity include acts of terrorism or serious organised crime such as human trafficking. The legislation must also specify realistic periods of data retention and provide sufficient safeguards into protecting rights of privacy and data protection.

Key Provisions in DRIPA

Section 1 DRIPA allows the Secretary of State to issue a notice to ISP and CSP's to retain relevant communications data (a retention notice) if the Secretary of State considers the requirement to be necessary and proportionate. Again similar qualifications as seen in RIPA must apply for the notice to be issued and they include the likes of national security, to prevent crime or disorder, the UK's economic interests, and the protection of public health.[75] Where these conditions exist the retention notice can relate to a particular operator or any description of operators where the notice will require the retention of all data or of the type described in the notice and specify the

[73] 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

[74] Ibid, p. 539

[75] S.1(1) Data Retention and investigatory Powers Act 204 and section 22(2) Regulation of Investigatory Powers Act 2000

period the data should be detained,[76] with the maximum period of data retention not exceeding 12 months.[77] In order to make requests on ISP and CSP's on a lawful footing, DRIPA has amended section 5 (3) RIPA (that is concerned with the grounds necessary for issuing of warrants to intercept communications) adding the issuing of a warrant is necessary where in the circumstances it appears to the Secretary of State the warrant is relevant to the interests of national security.[78]

Where a nation state legislates the granting of powers for the likes of retention notices and warrants is all well and good when applying to companies located within that state, but the law of one state is not normally applicable to companies located outside that state. As many ISP and CSP's are located outside the UK, it can in effect make these powers redundant. DRIPA has tried to address this issue by amending RIPA to allow for an interception warrant to be delivered at the company's principal office within the UK. If that company does not have a principal office at any place in the UK is where that company carries on their business or conducts its activities.[79] Should there still be non-compliance by that company located outside the UK to the warrant, DRIPA amends section 11 of RIPA to give effect that the warrant is enforceable by civil proceedings.[80] To assist in ensuring there are ways of improving the access of electronic communications data, the UK appointed its former US Ambassador, Sir Nigel Sheinwald as special envoy on intelligence and law enforcement data sharing. His role is lead discussions with key international partners and ISP and CSP's seeking to:

[76] S.1(2) Data Retention and Investigatory Powers Act 2014
[77] S1(5) Data retention and Investigatory Powers Act 2014
[78] S.3(2) Data Retention and Investigatory Powers Act 2014
[79] S4(2) Data Retention and Investigatory Powers Act 2014
[80] S.4(5) Data Retention and Investigatory Powers Act 2014

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.[81]

However DRIPA has a sunset clause where the Act is due to expire in December 2016 requiring the UK to either continue with this Act (following a House of Commons debate on the issue) or to let it expire and introduce a new Act.

The Investigatory Powers Bill: Is there a need for further legislation?

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 your family safe.'[82] 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;

[81] 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]
[82] 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]

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.[83]

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'[84]

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 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.' [85]

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

[83] 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]
[84] [n.38]
[85] 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]

Coalition who saw the proposed measures being too intrusive.[86] 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 under the conditions seen in RIPA and DRIPA (that is conditions such as national security or to prevent or detect crime and disorder). It is expected that similar clauses will be contained in the Investigatory Powers Bill.

It is hoped that the Investigatory Powers Bill will be a standalone piece of legislation repealing sections of RIPA, ISA and WTA providing sufficient safeguards in relation to rights to privacy and data protection. It is important the Bill is clear in what electronic communications is subject of surveillance to prevent any confusion and to appease citizens as to what type of and why certain communications are being examined by the intelligence and policing agencies. In addition to this to all surveillance authority applications must be specific as to why they are necessary, clearly stating the nature of the investigation and the grounds as to why such an authority is needed. It is also important that all authority applications are authorised by the judiciary not a Secretary of State. Anderson's 2015 report sums up why judicial authority should be sought as it would:

1. Improve public confidence;[87]
2. Judges' experience of police attitudes and methods renders them qualified to assess if an application is truly necessary (and the police have high professional respect for the judiciary; and

[86] [n.38]
[87] Anderson [n.62] p.270

3. It meets the requirements of the Digital Rights decision and ECHR regarding the requirements of data protection and rights to privacy.[88]

Conclusion

Returning to the question whether the UK needs a new piece of legislation governing surveillance of electronic communications data, it is submitted it does. While RIPA appears to contain wide surveillance power, the UK Parliament's ISC report on privacy and security described RIPA as, 'an analogue law in a digital age.[89] When RIPA was introduced in 2000 the use of electronic communications was limited compared to 2015. In 2000 there was no broadband facility, mobile phones allowed its users to telephone or text whereas to day the mobile phone is a small computer and of course social media did not exist in 2000. The ISA is also showing a sign of aging as legislation struggles to keep up with technology advances in communications. As most people's use of the internet ranges from a wide range of activities such as entertainment to shopping to banking carried out on various forms from personal computers, tablets and mobile phones, never before has the safety of data protection been so paramount. Therefore it is an imperative that Anderson's recommendation is included in that Investigatory Powers Bill by only allowing authorisations to be granted following judicial scrutiny. Equally important is the ability of the UK intelligence and policing agencies are granted powers of surveillance of electronic communications under one piece of legislation that is clear as to what can be monitored and is specific and proportionate to the investigation carried out by those agencies.

In the last twelve months we have witnessed a more sophisticated approach in the use of communications by terrorist groups. This has applied to Islamic State whose social media use has been very effective in communicating their messages to encourage others to join their cause, be it to travel to the caliphate to fight or live or in radicalising individuals to carry out

[88] Ibid p.271
[89] Intelligence and Security Committee of Parliament [n21, p.101

attacks outside the caliphate. Internet and communications service providers can play a vital role in assisting intelligence and policing agencies by retaining communications data they suspect to be linked to terrorist activity and pass this on. As stated, due to the current terrorist threat we have moved to an era form ‘need to know’ to ‘need to share’. This is important as these agencies need the tools to protect the most important of all human rights, the right to life of the citizens they serve. This should ensure that two key safety issues are protected, the safety of a person’s communications data and the safety of people’s lives.