Time to Re-Introduce a Directive on the use of Passenger Name Record Data

1. Introduction

In the last fifteen months Europe has witnessed three major terrorist attacks, two in Paris in January and November 2015 and in Brussels in March 2016 killing 179 people in total. Prior to all three attacks terrorists had travelled form, to and within the European Union (EU). In addition to this, a terrorist attack was prevented by passengers on a Thalys train travelling from Amsterdam to Paris. Apart from attacks, a high number of EU citizens have travelled to conflict zones such as the terrorist group Islamic State's self-proclaimed caliphate in Syria and Iraq, many of whom who have returned to EU Member States. In January 2015 the number of citizens from France, the UK, Germany and Belgium that travelled to join Islamic State was estimated to be 3,050 (BBC 2015), a number that has risen since then. As a result there have been calls for the EU to introduce a Passenger Name Record (PNR) data Directive to monitor passenger airline travel out of and to EU Member States.

PNR data transfer has not been without its problems and critique. This article will examine previous EU PNR agreements, mainly with the US, examining why they were problematic, with the main issue centring on the protection of passengers' personal data. In 2011 the EU attempted to introduce a PNR data Directive, but again this failed because there was insufficient safeguards protecting personal data. However, since 2011 there have been significant developments in the protection of personal data in the EU. This article will analyse two key decisions by the Court of Justice of the European Union (CJEU) in *Schrems* and *Digital Rights*. Both cases had a significant impact on personal data that resulted in the termination of a trade agreement between the EU and the US, and, the striking down of EU and Member State legislation governing surveillance and data retention of electronic communications. As the EU has developed significantly since 2001 in the area of justice and home affairs, this article will examine the current 2015 PNR data Directive assessing if it will

satisfy the strict EU legal restrictions on protection of personal data. Due to the current terrorist threat the EU and its Member States face, it is argued there is a need for a PNR data Directive and it is submitted the 2015 proposal balances correctly the needs of national security with the protection of personal data.

2. Previous EU PNR Transfer Agreements

Following Al Qaeda's attack on the US on the 11th September 2001 (9/11) where Al Qaeda operatives hijacked civil aviation aircraft and flew them into the World Trade Centre in New York and the Pentagon in Washington, the US called for tighter control on civil aviation travel. This included recording details of airline passenger through PNR data, which through the US' Aviation and Transport Security Act that was introduced in November 2001, became a statutory obligation. The Act required airline companies operating passenger flights to, from or through the US to provide US authorities with electronic access to PNR data that incudes passenger names and addresses, bank details, credit card details and information about meals ordered for flights (Kaunert, Leonard & McKenzie 2012, p.483). It was not until May 2004 when an agreement (Decision 2004/535/EC) was made to transfer PNR data from Europe to the US was agreed between the EU Commission and the US Department of Homeland Security (Argomaniz 2009 p.123). An obstacle for the EU in agreeing to the US requests for PNR data centred on the EU's obligation under article 25 of the1995 Data Protection Directive (Directive 95/46/EC) that the EU should not transfer data to another country that cannot guarantee an adequate level of protection is ensured (Argomaniz 2009, p.123, Kaunert et al., 2012, p.484).

Under the 1995 Directive EU Member States must ensure that personal data is processed fairly and lawfully (article 6(1)(a)). The Directive clearly states personal data can only be collected for specified, explicit and legitimate purpose and not be processed in a way

incompatible with these purposes (article 6(1)(b)). Member States can only derogate from the Directive where it is necessary to safeguard national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences (article 13(1)). Prior to any data exchange it is the Commission's responsibility to asses that the third country has an adequate level of protection of basic freedoms and rights of individuals (article 25(6)). Should the Commission find the third country does not provide an adequate level of protection, Member States are to take measures to prevent the transfer of data to the third country (article 25(4)). From the outset, one problem with the 2004 agreement was the duty on air carriers to provide PNR data, thereby placing them in a difficult situation. If they failed to pass on the PNR data to the US authorities they could face hefty fines or even lose their flying rights, but if they breached the 1995 Directive they could face fines from the EU (Kaunert et al. P.484) that could be up US$6,000 per passenger (Pawlak 2009, p.4).

The 2004 agreement was annulled by the CJEU in *European Parliament v European Council and Commission* 2006.[1] In reaching its decision the CJEU applied provisions contained in the 1995 Directive. However, the judgement does not really focus on issues related to data protection, rather whether the Directive's scope in processing personal data fell outside Community law.[2] Examining article 3(2) of the 1995 directive, the CJEU held as the sale of an airline ticket is a supply of a service, the collection of PNR data by airlines is an activity that falls within Community law, but the processing of that data that was regarded as being necessary for safeguarding public security and for law enforcement purposes resulted in the agreement being annulled. Referring to the earlier CJEU decision made six months earlier in *Lindqvist* 2003,[3] and applying the provisions of article 3(2) of the 1995 Directive that states the Directive does not apply top the processing of personal data in

[1] Joined cases C-317/04 and C-138/04
[2] *European Parliament v European Council and Commission,* paragraph 54
[3] Case C-101/01

operations related to public security, defence, state security and areas of criminal law,[4] the CJEU held the processing of PNR data by private companies falls outside the scope of the 1996 Directive (paragraph 59). Key to this decision was that the 2004 agreement was incorrectly based on EU transport policy (which was the first pillar of the EU under the Treaty of Union) rather than the third pillar[5] (which was justice and home affairs). As a result the CJEU did not address the issue of data protection guarantees by US authorities (Kaunert et al, p.485). A second PNR agreement between the EU and the US came into force in 2007 based on the collection and processing of the data for state security and criminal law (Kaunert et al, 2012, p.485), that was replaced with a third PNR agreement between the EU and the US in 2012. The EU Council announced the 2012 agreement's goal was to prevent, detect, investigate and prosecute terrorist offences and related crimes as well as to help with serious cross-border crimes (Council of European Union 2012).

2.1 Criticism of Previous EU PNR Agreements

In relation to EU PNR agreements there has been a degree of criticism. The main criticism is that in prioritising the expansion of counter-terrorism cooperation with third countries, especially the US, the EU was not so sensitive on data protection rules (Ilbiz, Kaunert and Anagnostakis. 2015, p.2). To some observers this has been more prevalent in the EU-US agreements than in EU negotiations with other third countries (Ilbiz et al. pp.8-13). In its building of network allies the EU's key partner has been the US, where in spite of divergent strategic cultures, judicial and data protection practices no other international actor has influenced EU policies more comprehensively than the US which has led to concerns about the impact of this collaboration on European citizens' privacy rights (Argomaniz 2012, p.95). To rationalise and provide an understanding why this is the case Lehrke and

[4] case C-317/04 and C-318/04, paragraph 58
[5] The three pillars formed under the 1993 Treaty of Union became annulled under the 2009 Treaty of Lisbon

Schomaker have developed the network hypothesis where the more embedded a country, or in this case the EU, is in networks through which the US could exert influence, the stronger is that country's counter-terrorism policy (2014, p.693). In applying this hypothesis Lehrke and Schomaker state that as the US has a presence in many different EU venues, the US was able to exercise influence of the Council and Commission (2014, p.698). This builds on Pawlak's earlier study. For Pawlak as the EU's security consciousness had not developed as rapidly as the US', the US had the opportunity exert a big influence on transatlantic agenda with the EU thereby dictating and shaping the EU's security agenda (2009, pp.9-10). Following the horrific Al Qaeda 9/11 attacks, the 2004 Madrid bombing and the 7/7 attacks in London in July 2005 it is understandable why the EU adopted the position they did. Addressing the threat posed by international Islamist groups EU bodies and agencies realised the need to be supportive in the international co-operation required to counter these groups posed to international security. In the early years of the 21st century the Justice and Home Affairs Commission and its related bodies such as its policing agency Europol were still in their infancy and developing. One can see how and why the US took advantage of the EU's relative unpreparedness to counter terrorist threats. In fact prior to the 2009 Treaty of Lisbon Europol had to sell to EU Member States projects that must given priority whereas today projects are developed with Member States that are in line with Europol's overall strategy (Busuoic and Groenleer 2013, p.293). As will be discussed, this change of position will underpin the submission that an EU PNR Directive would not be led by or under the influence of US policy and legalisation. In maintaining a strong position in protecting personal data, the fear of antagonising third countries has virtually evaporated as seen with recent CJEU decisions.

3. The EU's Directive on Passenger Name Records 2011/0023

In 2015 the EU considered introducing a PNR data Directive, but it was not the first time the EU considered this. In February 2011 the European Commission produced a proposal for a PNR data Directive for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (2011/0023). At the time of its publication the explanatory memorandum drew a distinction between PNR data and aircraft passenger information (API)) stating that PNR data would be more effective in assisting agencies investigating terrorism and serious crime. Key to this is PNR data contains more information than API. While API contains a passenger's name, date of birth, gender, nationality and passport details PNR data contains the following information:

- Name of Passenger;
- Contact details for the travel agent or airline office;
- Ticketing details;
- Itinerary of at least one segment, which must be the same for all passengers listed;
- Name of person providing the information or making the booking;
- Passenger gender;
- Passport details (includes nationality, passport number and date of passport expiry);
- Date and place of birth;
- Billing information;
- Form of payment (include debit/credit card details);
- Contact details (potentially include landline/mobile phone numbers);
- Frequent flyer data; and
- Vendor remarks kept by the airline (International Civil Aviation Organisation (2010) Guidelines on Passenger Name Record (PNR) Data Quebec: International Civil Aviation organisation).

API information was seen as restrictive by the European Commission who in the explanatory memorandum to the 2011 PNR Directive stated:

> 'API data does not enable law enforcement authorities to conduct an assessment of passengers and therefore do not facilitate the detection of hitherto "unknown" criminals or *terrorists*.' [my emphasis] (2011/0023 Directive p.7).

As PNR data contains wider information such as ascertaining who made the booking or contact details and methods of payment, this can be cross-checked by agencies making it

easier for their investigating officers to identify connections with terrorist suspects or criminals already in their intelligence systems.

3.1. Concerns Regarding the 2011 PNR Directive

The main concern with the proposed PNR data Directive was the sufficiency of protection of personal data especially in relation to the transfer of PNR data to third countries. In addressing this point the proposed period of detention of PNR data by a competent authority in the Directive was 30 days, with the Passenger Information Unit to retain the data for five years (Directive 2011/0023, article 9). In addition to the conditions laid down by the 1995 Data Protection Directive, it was considered there was additional protection of personal data through the Justice and Home affairs Council Framework Decision regarding the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[6] Under the Framework Decision the data subject has the right to expect the competent authority to fulfil its duties,[7] which includes the right for the data subject to have a judicial remedy for any breach of the rights guaranteed to them by the applicable national law.[8] Where PNR data is transferred to a third country once more the adequacy of data protection is mentioned as the Framework Decision is clear that prior to transfer of data from the EU the third country must have an adequate level of protection of the intended data processing.[9] Even though these safeguards were mentioned, the European Parliament expressed concerns regarding the proposed method of automatically processing PNR data using fact based pre-determined assessment criteria was very wide and thought that such an assessment should never result in , "…profiling on the basis of sensitive data" (Directive 2011/0023, Memorandum, p.10). In 2011 the European Data Protection Supervisor

[6] FD 2008/977/JHA
[7] FD 2008/997/JHA, article 18
[8] FD 2008/997/JHA, article 20
[9] FD 2008/997/JHA, article 14

questioned if the PNR data Directive was necessary and proportionate as he saw in the Directive insufficient protection of the individual's data privacy, a move he saw as contributing towards a surveillance society (Directive 2011/0023, Memorandum, p.10).

4. The EU Adopts a Hard Line on Privacy: CJEU Decisions Related to Data Protection

It is unfortunate that in *European Parliament v European Council and Commission* the CJEU did not address the question regarding the adequacy of data protection in third countries the EU makes agreements with, as the US has little in the way of legislative protection related to personal data. As Sotto and Simpson observe, the US legislative framework designed to protect personal data resembles a 'patchwork quilt' (2014, p.191). The lack of legal protection of personal data in the US has recently led to the EU annulling trade agreements, from which the CJEU decisions can be applied to PNR data exchange in any new directive.

4.1 EU-US Trade Agreement: Safe-Harbour

To protect EU citizens' personal data the EU-US Safe Harbour agreement was signed in 2000 under Decision 2000/520/EC in order to provide a streamlined process for US companies to comply with the 1995 Data Protection Directive. Among the privacy principles in the agreement it states that organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.[10] If US organisations flout EU privacy law the EU Commission can reverse the decision to grant the Safe Harbour arrangement.[11] The agreement was mainly aimed at the private sector's access to personal data for business purposes, but in November 2013 the

[10] Annex I, paragraph 12 Dec 2000/520, Export.gov, US-EU Safe Harbor Overview at http://www.export.gov/safeharbor/eu/eg_main_018476.asp [accessed 23rd September 2015]
[11]Art 3(4) Dec 2000/520European Commission, How will 'safe harbor' arrangement for personal data transfer to the US work? (09/10/2012) at http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm [accessed 23rd September 2015]

European Commission expressed concerns over the large scale access by US Intelligence agencies to data transferred by Safe-Harbour certified companies (European Commission 2013, p.18). This concern came from the disclosure and revelations by former employee of the US intelligence agency, National Security Agency (NSA), Edward Snowden that the NSA was involved in bulk data collection that included many EU citizens (Greenwld 2014, p.92). This led to the European Commission stressing the importance of the national security exception in the Safe-Harbour Decision should only be used when it is, '…strictly necessary or proportionate'.[12] If the EU's legal legitimacy credentials are to be measured, it is in the CJEU's judicial interpretation and decisions that demonstrates how data protection is deeply embedded in EU law.

4.2 *Schrems* Case

Schrems, an Austrian citizen, used the social media network, Facebook, since 2008. Although his contract was registered within the EU at the time of his registration with Facebook Ireland, this is a subsidiary of Facebook Incorporated which is established in the US, where Facebook Ireland users' personal data is then transferred to the US. Schrems contended that the law and practice in the US did not ensure sufficient protection of his personal data and in referring to the Snowden revelations of NSA practices, he claimed his personal data could have been subject to retention by the NSA and other US federal agencies.[13] Perceiving Schrems' complaint as unsustainable in law and bound to fail because he saw it as vexatious, the Irish Data Protection Commissioner did not see himself as being required to investigate the complaint as there was no evidence that Schrems' personal data had been accessed by the NSA.[14] In Schrems' judicial review of the Irish Commissioner's

[12] Dec 2000/520, p.19
[13] Ibid, paragraphs [26] – [30]
[14] *Maximillian Schrems v Data Protection Commissioner* Case C-362/14 (Advocate General Opinion - delivered 23rd September 2015), paragraph [30]

decision,[15] the Irish High Court held once personal data has been transferred to the US it is capable of being accessed by the NSA and other US federal agencies in the course of indiscriminate surveillance and interception of communications.[16] Justice Hogan said if this matter was to be measured solely by Irish law and Irish constitutional standards a serious issue would arise which the Commissioner would have been required to investigate whether US law and practice in relation to privacy, interception and surveillance matched those standards.[17] Acknowledging the Snowden revelations had exposed 'gaping holes' in contemporary US data protection practice,[18] Justice Hogan did not see Schrems' complaint as 'frivolous or vexatious'[19]and refereed it to the CJEU.

Advocate General Bot held that as intervention of independent supervisory authorities is at the heart of the EU's system of personal data protection, there must be a similar system of protection in the third country to which the data flows from the EU.[20] In this case under the US' surveillance Act, Foreign Intelligence Surveillance Act 1978, the NSA accessed personal data inputted in Austria that was held by Facebook at a server in the US. Advocate General Bot held that the Foreign Intelligence Surveillance Court does not offer an effective judicial remedy to EU citizens whose personal data has been transferred to the US.[21] He proposed that when the case went to the CJEU it should answer the question if the agreement is invalid.[22] The CJEU did answer this question and declared the 2000/520 Decision as invalid[23] and consequently brought to an end the Safe Harbour Agreement. Crucial to the Court reaching this decision were the requirements of article 25 of the 95/46 Directive on data

[15] *Maximillian Schrems v Data Protection Commissioner* [2014] IEHC 310
[16] Ibid, paragraph [14]
[17] Ibid, paragraph [79]
[18] Ibid, paragraph[69]
[19] Ibid, paragraph [74]
[20] n 9, paragraph [210]
[21] Ibid, at [210] and [211]
[22] Ibid, at [237]
[23] n 1, paragraph [107]

protection. Where communications data is transferred from outside the EU to a third country, the EU is responsible for ensuring the third country has an adequate level of data protection. In doing so, consideration is given to the nature of the data, the purpose and duration of the processing operation of the data, the country of origin and final country of destination, the law in operation related to data protection in the third country and the professional rules and security measures deployed regarding the data in the third country.[24]

The most pertinent part of article 25 related to the issue in *Schrems* is it being the Commission's responsibility to find that the third country ensures an adequate level of protection of basic freedoms and rights of individuals.[25] Should the Commission find the third country does not provide an adequate level of protection, Member States are to take measures to prevent the transfer of data to the third country.[26] Crucial to determining this is what is meant by the term 'adequate'. The third country is not required to ensure there is a level of data protection identical to that guaranteed in EU law,[27] Advocate General Bot said that the protection implemented by the third country may differ from EU law, but it must provide adequate protection that is equivalent to that afforded by the 95/46 Directive.[28] Adopting the linguistic viewpoint of the word 'adequate' which means satisfactory or sufficient, Advocate General Bot said the obligation of the Commission is to ensure the third country has a sufficiently high level of protection of fundamental rights.[29] The obligation to ensure the adequacy of data protection is not a one-off obligation made at the time of agreement. The obligation for the third country is an ongoing obligation to ensure that no changes in circumstances arise that can call into question the initial assessment[30] and it is

[24] art 25(2) Directive 95/46/EC
[25] Ibid, art 25(6)
[26] Ibid, art 25(4)
[27] n 1, paragraph [73]
[28] n 9, paragraph [141]
[29] Ibid, paragraph [142]
[30] Ibid, paragraph [147]

expected the Commission will regularly review the third country's level of protection.[31] It was on this legal point that Schrems was successful as the CJEU found the 2000 Decision did not cover the situation to limit interference by US state bodies authorised under legitimate objectives, such as national security, in US law to interfere with personal data transferred from the EU.[32] The Court added that legislation permitting public authorities access to the content of electronic communications on a *generalised basis* must be regarded as compromising the essence of the fundamental right to privacy under the CFRF.[33] On the latter point, the CJEU found there to be no effective remedy for an individual ensure the data was used in compliance with legal provisions similar to those found in the EU.[34]The main surprise from *Schrems* is not in finding that the Safe Harbour Agreement was ruled as invalid, with such gaping holes in US privacy law and lack of protection of personal data is that this Agreement lasted for fifteen years.

It may come as a surprise that the US has no legislation that deeply embeds data protection within its legal system. Other western states that have agreements with the EU appear to apply similar legal principles in relation to data protection. For example the US' northern neighbour, Canada has the Privacy Act 1985 as well as Personal Information Protection and Electronic Documents Act 2000, the latter being concerned solely with the use of electronically stored personal data. Both Acts are clear that personal information cannot be used unless it meets strict criteria[35] similar to the provisions in the 95/46 Directive and both Acts also have sufficient safeguards where individuals can make complaints to the Privacy

[31] Ibid, paragraph [137], n6, paragraph [76]
[32] n 1, paragraph [88]
[33] Ibid, paragraph [94]
[34] Ibid, paragraph [95]
[35] s.7 Privacy Act (1985 (Canada), s.4 Personal Information Protection and Electronic Documents Act 2000 (Canada)

Commissioner[36] and the Canadian courts.[37] Likewise the Australia's Privacy Act 1988 contains similar provisions as the Canadian legislation with section 7 promoting the privacy of an individual's personal data with the safeguards including complaints to the Australian Privacy Commissioner[38] or to an Australian Court.[39] As both Canada and Australia have agreements with the EU regarding the processing and transfer of passenger name record data held by air carriers[40] the two respective states' legislation clearly offers a level of protection equivalent to that afforded by the 95/46 Directive. The decisions in *Digital Rights* and *Schrems* demonstrates how EU law views the importance in protecting personal data and why it is best placed as an international actor to encourage those third countries it has agreements with to adopt similar measure in relation to data protection.

4.3 *Digital Rights* Case

How CJEU decisions impact on EU and Member States' law was seen in *Digital Rights Ireland*[41] where the Court ruled that an EU Directive was invalid.[42] The case centred mainly on Directive 2006/24/EC that laid down an obligation on publicly available electronic communications services or public communications networks to retain certain data generated or processed by them. As collaboration between EU Member States was seen as critical, the Directive was introduced following the Al Qaeda attack in London 2005 with the intention to facilitate the exchange of personal data in order to enhance the prevention capabilities regarding acts of terrorism and crime (Bignami 2007, p.237). The 2006 Directive was also introduced to shift data protection rights from national to EU level thereby ensuring the

[36] Ibid, s.29, s.11
[37] Ibid, s.34, s.46
[38] s. 34 Privacy Act 1988 (Australia)
[39] Ibid, s.46
[40] Agreement (Canada) L 82/15, Agreement Australia L 186/4
[41] Digital Rights [2014]EUECJ C-293/12, [2014] 3 WLR 1607
[42] Ibid, paragraph [71]

police and the judiciary in one Member State respect the data protection rights in another Member State.[43] As the Directive allowed EU Member States' intelligence and policing agencies to collect bulk data, the CJEU examined the acceptable limits of mass surveillance and the function of data protection (Roberts 2015, p.538) in relation to compatibility with articles 7 and 8 EU's Charter of Fundamental Rights and Freedoms (CFRF). Regarding data protection the CJEU found the 2006 Directive to be invalid. Key to this decision was article 4 of the Directive allowing Member States to adopt into its national law measures ensuring that data retention is provided only to the competent national authorities in specific cases.

In *Digital Rights* the CJEU saw two key legal issues as important to ensure personal data is protected:

1. EU legislation must lay down clear and precise rules governing the scope and application of the measure in question, especially in relation to access to and use of personal data;
2. Minimum safeguards are imposed to provide sufficient guarantees effectively protecting personal data against the risk of abuse and against unlawful access and use.[44]

Analysing the inadequacies of article 4 in the 2006 Directive, the CJEU held it 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.[45] The CJEU these data retention measures were too vague, as the principles of necessity alone cannot justify imposing limitations on citizens' rights.[46] While acknowledging that data retention is an important strand in terrorism and serious crime investigations to ensure public safety and it is

[43] Ibid, pp.234-236
[44] Digital Rights [2014]EUECJ C-293/12, [2014] 3 WLR 1607 at [54]
[45] Ibid at [61]
[46] Ibid at [66]

in these specific grounds there could be a justification,[47] in *Digital Rights* the CJEU has made it clear that the protection of personal data is equally important. The *Digital Rights* decision is not a 'total knockout' to mandatory retention (Ojanen, 2014, p.539). 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, specifying realistic periods of data retention and sufficient safeguards into protecting rights of privacy and data protection would be sufficient. What the *Digital Rights* decision does is impose on the EU and member States' legislators a new level of responsibility to protect fundamental rights, it composes substantive instructions for law-makers at EU and national level to guarantee the protection of data protection and, importantly, provides a strict judicial scrutiny test (Granger and Irion 2014, p.849).

The impact of *Digital Rights* is seen in a number of Member states. In the UK *R (on the application of Davis and ors) v Secretary of State for the Home Department and ors*[48] the High Court examined the provisions of data retention and how it balances with the protection of personal data in the Data Retention and Investigatory Powers Act 2014 (DRIPA) that was introduced by the UK government in response to the *Digital Rights* decision, Following the CJEU's decision in *Digital Rights* he High Court held that regardless of the changes the UK Government made in relation to data retention, DRIPA still failed to provide sufficient safeguards against unlawful access to and use of retained data by public authorities and as such the Act infringed the principle of proportionality.[49] Lord Justice Bean made it clear that in protecting fundamental rights in relation to personal data, derogations and limitations to that right must only occur when it is strictly necessary and this can only be achieved if legislation lays down clear and precise rules governing the scope of that derogation and

[47] Ibid at [51]
[48] [2015] EWHC 2092 (Admin)
[49] Ibid, at [88]

limitation.[50] He also added that sufficient safeguards should be imposed in order to give sufficient protection against the risk of abuse or unlawful access to that data. In saying this, he stressed the point that legislation permitting a general retention of personal data must expressly be restricted to the purpose of preventing, detecting, or, conducting prosecutions for serious offences.[51]

In March 2015 a national Dutch court in The Hague followed the CJEU and found Holland's surveillance and data retention law fell under the EU law and the CFRF. As the Dutch law failed to conform adequately to articles 7 and 8 of the CFRF, along with the court also finding insufficient safeguards, the Court suspended the Dutch law (Meyer 2015). Similar legal issues were found in the respective domestic statutory provisions regarding surveillance of communications post-*Digital Rights* by the respective judiciaries in Sweden, Romania and Belgium where their respective courts have held their legislation to be in breach of EU law.[52] All of the Member State domestic court findings centred on two key legal points raised in *Digital Rights*, which are vague provisions to access and retain communications data and the lack of sufficient safeguards protecting potential abuse in the use of that data. From these court decisions it is clear that to achieve sufficient safeguards of data protection, the responsibility must be taken from politicians and placed with the judiciary or totally independent bodies.

4.4 Main Points from the Schrems and Digital Rights Decisions

What we witness with both of these cases is how the EU is maturing and becoming stronger in challenging legislation, agreements and decisions that impact on EU citizens'

[50] Ibid at [91a]
[51] Ibid at [91b]
[52] *R (on the application of Davis and ors) v Secretary of State for the Home Department and ors*, [2015] EWHC 2092 (Admin), paragraph [111]

personal data. The *Schrems* case in particular demonstrates the moral courage of the EU's judiciary to declare that arguably the most powerful economic state, the US' law on privacy is lacking sufficient protection and is inadequate to handle EU citizens' personal data thereby ending an important economic trade agreement. As a result of the CJEU's decision in *Schrems* the Safe-Harbour Agreement was swiftly been replaced by the EU-US Privacy Shield where the US is committed to ensuring the US public authorities access to personal data will be subject to clear conditions, limitations and oversight, preventing generalised access with a complaint system to a dedicated new Ombudsman (European Commission Press Release 2016). This demonstrates how the EU's standing as an influential and important international actor is increasing and maybe suggests that there has been a power shift from that discussed with the early EU-US PNR agreements that suggested that the power laid with the US. As we enter the second decade of the 21st century decisions like that seen in *Schrems* suggest that there is at least parity in the power paradigm between the EU and the US.

The *Digital Rights* decision is equally important as the decision covers more than striking out one EU Directive, it impacted on legislation within the Member States. More importantly it set down a legal marker for all legislation and legal instruments to adhere to on issues around necessity, proportionality and importantly having specific reasons as to why statutory power should be given to state authorities to interfere with citizens' personal data. This underpins agreements made by EU bodies and agencies with third countries. Another impact the *Digital Rights* decision has had in relation to EU legal instruments is in bringing to the fore the importence of adherence by the EU bodies and agencies as well as the Member States to the CFRF. While acting in a manner compatible with the European Convention of Human Rights which all EU Member States must signed up to, certainly post Digital Rights they must act in a manner than complies with the CFRF.

5. 2015 Proposed New Version of a PNR Directive

A new draft text on an EU system for the use of PNR data was tabled by Timothy Kirkhope MEP which was discussed in the LIBE Committee on 26 February 2015 (Bakowski and Voronova 2015, p.4). An evaluation of the necessity and proportionality of the proposal in the face of current security threats, its scope (list of offences covered), retention periods, the inclusion or exclusion of intra-EU flights, the connection with the on-going data protection reform, as well as the consequences of the CJEU judgment in *Digital Rights*, were among the issues discussed by MEPs.

The changes proposed in the revised draft report include:

- The scope of the proposal is narrowed to cover terrorist offences and serious "transnational" crime (the list of specific offences includes, for instance, trafficking in human beings, child pornography, trafficking in weapons, munitions and explosives);
- Sensitive data to be permanently deleted no later than 30 days from the last receipt of PNR containing such data by competent authorities. Other data will continue to be masked after 30 days;
- The inclusion of intra-EU flights (not initially included by the Commission, but the Council of the European Union favours the inclusion of internal EU flights);
- 100% coverage of flights (the Commission text proposed to reach 100% coverage of international flights in gradual steps);
- Access to the PNR data continues to be allowed for five years for terrorism, but is reduced to four years for serious crime;
- Each EU Member State should appoint a data protection supervisory officer;
- Persons who operate security controls, who access and analyse the PNR data, and operate the data logs, must be security cleared, and security trained;
- The period for Member States to transpose the directive is extended from two to three years (given the specific technological and structural demands of setting up an EU PNR system for each Member State) (Bakowski and Voronova 2015 pp.4-5).

In addition to the terrorist attacks in Paris in January 2015, the Islamic Sate attacks in Paris on the 13th November 2015 may have accelerated movement by EU officials in relation to the 2015 PNR Directive proposal as on the 4th December 2015 the Council of the European union moved swiftly to endorse the PNR Directive proposal that was approved by the European Parliaments' Civil Liberties, Justice and Home Affairs committee with a vote due in the

European Parliament in early 2016 (Papademetriou 2015). As the passenger movement to and from and within the EU has not just been with aircraft it is suggested that the Directive be amended to include inter-state rail and ship travel.

4.1 European Data Protection Supervisor's Concerns Over the 2015 PDR Directive Proposal

In September 2015 the European Data Protection Supervisor (EDPS) published his opinion on the 2015 PNR data Directive. While in general he welcomed the improvements made by the European Council and civil liberties LIBE Committee on the provisions contained in the Directive regarding the provisions on data protection (EDPS Opinion 2015, p.15), he still has some reservations. On bulk and indiscriminate collection of data he recognised that PNR data would cover at least all flights to and from the EU concerning more than 300 million non-suspect passenger a year. The EDPS recommended that the Directive ensure that the data obtained pertained to a particular time period, geographical zone and a circle of particular persons likely to be involved in terrorism and serious crime (EDPS Opinion 2015, p.7). In addition to recommending that the data retention period be shorter than five years he is sceptical that the rationale to obtain PNR data under the notion of immediate and serious threat to public security or serious transnational crimes is sufficiently specific to meet the standards set in the *Digital Rights* decision (EDPS Opinion 2015, p.13).

To help allay some of these concerns could be the role Europol plays. The EDPS recommends that the Member State agencies responsible for dealing with PNR data align themselves with the regime applicable to Europol to restrict conditions of access to the PNR data processed by the EU (EDPS Opinion, p.13). This is a logical step. Firstly Europol is subject of judicial scrutiny as post 2009 Treaty of Lisbon Europol's actions are subject to judicial review by the CJEU (Busuioc and Groenleer 2013, p.299) and this would help ensure legal redress by citizens who are concerned their data has misused. The Treaty of Lisbon has

not just ensured there is solely judicial scrutiny of its actions, the Treaty also affords the European Parliament as well as national parliaments authority over Europol (Occhipinti 2015, p.246) In addition to this Europol's counter-terrorism role has gown,. Helping this growth has been Europol's permanent unit of experts to provide national authorities with analysis and support. In addition to this Europol staff members have become increasingly important as project managers for its analytical work files that are being used more extensively because Europol has proven that its information sharing systems can be trusted to protect personal data (Occhpinti 2015, pp.239-241). Another key development in Europol has been the creation of the European Counter-Terrorism Centre (ECTC) where one of the aims of the ECTC is to improve information exchange between Member States' law enforcement agencies. On the ECTC, Europol's Director, Rob Wainwright said:

> 'Our ambition is for the European Counter Terrorism Centre to become a central information hub in the fight against terrorism in the EU, providing analysis for ongoing investigations and contributing to a coordinated reaction in the event of major terrorist attacks. Europol is grateful for the support of the Member States, the European Parliament and the European Commission in the establishment of the ECTC. It will lie at the heart of a stronger EU standing up to the threat of terrorism.' (Europol 2016)

As Europol has the staff, resources and departments that are legally accountable thereby ensuring compliance with EU personal data law, this will enable Europol to scrutinise requests for PNR data on a case-by-case basis. With Europol scrutinising and co-ordination the transfer of PNR data, it will ensure that on the limited circumstances where there is sharing of the data with third countries it will go some way to protecting EU citizens' personal data.

6. Conclusion

With the current terrorist threat facing many EU Member States it is of paramount importance that a PNR data Directive is introduced. As has been argued above, in recent years the EU has demonstrated it has the legal responsibility to protect personal data. This is important due to the high volume of passengers travelling to and from, as well as within the EU. Equally important is that to prevent any data mining that PNR data requests are closely monitored and controlled as the vast majority of passenger will be literally innocent travellers with no connections to terrorism or serious international criminal activity. Equally important is ensuring the needs of national security are also met. As stated, in the past fifteen months179 citizens have been killed in three terrorist attacks with many more seriosuly injured. The purpose of PNR data requests by relevant authorities is to prevent any further attacks and protect people from death or serious injury. Since 2001 when it was shown any PNR agreements were based on terms of third countries not the EU's legal foundation, this situation has changed as seen in the *Schrems* decision where in protecting EU citizens' personal data the CJEU had the courage to make a decision knowing it would terminate an important trade agreement between the US and the EU. A positive taken from that is a new agreement was quickly reached that did tighten up the protection of EU citizens' personal data with the US. The EU also has its agencies like Europol, whose recent standing has been enhanced and can trusted to ensure that any PNR data request are strictly controlled on a case-by-case basis> Tis not only ensures the protection of personal data is secure, but importantly, Europol can also ensure the needs of security measures are also met. If there is one area where the PNR data Directive could be enhanced it would be to include inter-state rail and ship travel as the Thalys train incident in August 2015 showed, terrorists do not just use air travel. While the Directive will not totally stop terrorists travelling into and out of Europe, this Directive can help as a deterrent to terrorists using these modes of transport thereby ensuring the safety of passenger and to enhance the safety of EU citizens as a whole.

References

Export.gov, US-EU Safe Harbor Overview Annex I, paragraph 12 Dec 2000/520 retrieved from http://www.export.gov/safeharbor/eu/eg_main_018476.asp [accessed 23rd September 2015]

Argomaniz, J. (2009) When the EU in the 'Norm-taker': the Passenger Name records Agreement and the EU's Internalisation of US Border Security Norms *Journal of European Integration* 31(1), 119-136

Argomaniz, J. (2012) *The EU and Countger0terrorism: Politics, polity and policies after 9/11* London Routledge

BBC News (2015) 'Terror threat posed by thousands of EU nationals' retrieved on 22nd January 2015 from http://www.bbc.co.uk/news/uk-30799637

Bignami, F. (2007) Privacy and Law Enforcement in the European Union: The Data Retention Directive *Chicago Journal of International Law* 8(1) 233 - 251

Busuioc, M. and Groenleer, M. (2013) beyond Design: The Evolution of Europol and Eurojust *Perspectives of European Politics and Society* 14(3), 285-304

Connelly, C. (2008) 'The US Safe Harbor – Fact or Fiction?'Galexia Pty Ltd

Council of the European Union (2012) Council adopts new EU-US agreement on passenger Name Records (PNR), 9186/12, PRESSE 173, retrieved 4th March 2016 from http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf

EDPS Opinion (2015) Second opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger name record data for the prevention, detection, investigation and prosecution of terrorist and serious crime retrieved 14th March 2016 from https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf

European Commission (2013) Communication on the Functioning of the Safe-Harbour from the Perspectives of EU Citizens and Companies Established in the US, COM(2013)847 Final,

European Commission (2012), Art 3(4) Dec 2000/520, How will 'safe harbor' arrangement for personal data transfer to the US work? (09/10/2012) retrieved from http://ec.europa.eu/justice/policies/privacy/thridcountries/adequacy-faq1_en.htm [accessed 23rd September 2015]

European Commission Press Release (2016) EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2nd February 2016, retrieved 6th March 2016 from http://europa.eu/rapid/press-release_IP-16-216_en.htm

Europol (2016) Europol's European Counter terrorism Centre Strengthens the EU's Response to Terror, 25th January 2016 retrieved 4th March 2016 from https://www.europol.europa.eu/content/ectc

Bakowski, P and Voronova, S. (2015) The proposed EU passenger name record (PNR) directive: Revived in the new security context, Euroepan Parliament Briefing, April 2015, retrieved 9th March 2016 from http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf

Granger, M. and K. Irion, K. (2014) The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection *European Law Review* 39(6) 835-854

Greenwald, G. (2014) No Place to Hide: Edward Snowden, the NSA and the US Surveillance State New York: Metropolitan Books

Haynes, D. (2015) End of Safe Harbour isn't the end of the world – let's hope its successor is better *The Conversation* 12th October 2015, retrieved13th October 2015 from http://theconversation.com/end-of-safe-harbour-isnt-the-end-of-the-world-lets-hope-its-successor-is-better-48841

Ilbiz, E, Kaunert, C & Anagnostakis, D. (2015) The counterterrorism agreements of Europol with third countries: data protection and power asymmetry *Terrorism and Political Violence* DOI:10.1080/09546553.1092438

Kaunert, C., Leonard, S., and McKenzie, A (2012) The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT *European Security* 21:4, 474-496

Kelion, L.(2015) 'Facebook data transfers threatened by Safe Harbour ruling' BBC News 6th October 2015, retrieved 6th October 2015 from http://www.bbc.co.uk/news/technology-34442618

Lehrke, J.P. and Schmaker, R. (2014) Mechanisms of Convergence in Domestic Counterterrorism Regulations: American Influence, Domestic Networks and International Networks *Studies in Conflict & Terrorism* 37(8), 689-712

Meyer, D. (2015) Dutch court suspends metadata surveillance law over privacy (techeu 11th March 2015) retrieved 20th August 2015 from http://tech.eu/news/dutch-court-suspends-data-retention-law/

Muir, A. and Oppenheim, C. (2002) 'National Information Policy developments worldwide IV: copyright, freedom of Information and data protection' (2002) *Journal of Information Science* (28) 467-482

Ochipinti, J.D. (2015) Still Moving Towards a European FBI? Re-Examining the Politics of EU Police Cooperation *Intelligence and National Security* 30(2), 234-258

Ojanen, T. (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- 546

Papademetriou, T. (2015) European Union: Draft Directive on Collection and Transfer of Air Passenger Record data, 23rd December 2015 Library of Congress retrieved 9th March 2016 from http://www.loc.gov/law/foreign-news/article/european-union-draft-directive-on-collection-and-transfer-of-air-passenger-record-data/

Pawlak, P. (2009) Made in the USA? The Influence of the US on the EU's Data Protection Regime *CEPS – Liberty and Security in Europe*, retrieved from Centre for European Policy Studies website 7th March 2016 http://aei.pitt.edu/15102/1/made-usa-influence-us-eus-data-protection-regime.pdf

Roberts, A. (2015) Privacy, Data Retention and Domination: Digital Rights Ireland Ltd v Minister for Communications *Modern Law Review* 78, 522-543

Sotto, L.J. and A.P. Simpson, AJ, (2014) United States in Jay, R.P. (editor), *Data Protection & Privacy in 26 jurisdictions worldwide* (pp.191-208) London: Law Business Research