The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit For Purpose?

Abstract

In 2016 the EU introduced a Passenger Name Record data (PNR) Directive. In the EU there has been controversy over the acquisition and sharing of PNR data, related mainly to lack of safeguards and protection of personal data protection. This article examines these issues related to earlier EU PNR agreements with third countries and why previous EU attempts to legislate in this area failed. By drawing a comparison with the 2011 PNR Directive proposal, the article argues that by meeting the strict EU law on data protection as well as being necessary to assist in preventing and detecting acts of terrorism and serious crime it is submitted the 2016 Directive is fit for purpose and able to withstand scrutiny by the Court of Justice of the European Union.

Key Words

Passenger Name Records, Terrorism, Serious Crime, Digital Rights, Schrems, Surveillance Society

1.Introduction

In April 2016 the European Union (EU) introduced its Passenger Name Record (PNR) Data Directive to be incorporated into Member States' national law by the 25th May 2018.[1] Allowing relevant agencies access to PNR data related to air travel, the Directive's main aim is to prevent, detect, investigate and prosecute terrorism and serious crime.[2] This is the EU's second attempt at introducing a PNR Data Directive as their earlier proposal for a PNR Data Directive in 2011 failed on the grounds it had insufficient protection to safeguard an individual's data privacy.[3] However, recent events have necessitated the re-introduction of a PNR data Directive. In the last eighteen months Europe has witnessed three major terrorist

[1] Directive 2106/681, article 18(1).
[2] Directive 2016/681, para. (2).
[3] European Commission (2011) '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 offences and serious crime' COM(2011) 32 final <http://ec.europa.eu/home-affairs/news/intro/docs/com_2011_32_en.pdf> , 5th May 2016.

attacks, January[4] and November 2015[5] in Paris and in Brussels in March 2016[6] killing 179 people in total. Prior to all three attacks terrorists travelled from, to, outside and within countries in the EU. In addition to this, in August 2015 a terrorist attack was prevented by passengers on a Thalys train travelling from Amsterdam to Paris.[7] Apart from the terrorist attacks, a high number of EU citizens have used air travel as part of their journey 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,[8] a number that has risen since then. As a result there have been calls for the EU to introduce a PNR Data Directive to monitor passenger airline travel out of and to EU Member States.

Although the EU has now introduced legislation related to the acquisition and exchange of PNR data, this has not been a straight forward process. From looking at the rationale behind the requirement for PNR data, this article examines the issues and problems related to previous EU agreements with third countries over PNR data exchange and the EU's earlier attempts to introduce legislation in this area. The main stumbling block in reaching successful agreements and the introduction of legislation has been in ensuring the adequacy of protection of passengers' personal data. This emanates from a fear of expanding a surveillance society. The article examines EU data protection laws and judgements from the

[4] BBC News (2015) 'Charlie Hebdo attack: three days of terror', 14th January 2015, http://www.bbc.co.uk/news/world-europe-30708237>, 4th March 2016.
[5] C. Phipps and K. Rawlinson (2015) 'Paris attacks kill more than 120 people – as it happened', *The Guardian*, 14th November 2015, <https://www.theguardian.com/world/live/2015/nov/13/shootings-reported-in-eastern-paris-live>, 4th March 2016.
[6] BBC News (2016) 'Brussels explosions: what we know about airport and metro attacks', 9th April 2016, http://www.bbc.co.uk/news/world-europe-35869985>, 10th April 2016.
[7] A. Chrisafis (2015) 'France train attack: Americans overpower gunman on Paris express', 22nd August 2015, < https://www.theguardian.com/world/2015/aug/21/amsterdam-paris-train-gunman-france>, *The Guardian*, 4th March 2016.
[8] BBC News (2015) 'Terror threat posed by thousands of EU nationals', 13th January 2015, <http://www.bbc.co.uk/news/uk-30799637>, 25th January 2015.

Court of Justice of the European Union (CJEU) related to data protection as this is a key benchmark to assess if PNR data legislation is fit for purpose. In drawing a comparison between the 2011 proposal and 2016 Directive, the article argues that following key CJEU decisions related to EU data protection law there are much wider provisions in the 2016 Directive in relation to safeguards and the protection of personal data. This is in addition to assessing the necessity of the directive in relation to preventing terrorism, leading to an examination whether the Directive is sufficiently robust to withstand legal challenges. In conclusion the article argues the legislators have learnt from earlier experiences and by including greater width of data protection provisions, along with it still being necessary, the 2016 directive is fit for purpose.

2. The Rationale Behind the Requirement for PNR Data

Following Al Qaeda's attack on the US on the 11th September 2001 (9/11) where terrorists associated with Al Qaeda 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 passengers through PNR data, which through the US' Aviation and Transport Security Act 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 includes passenger names and addresses, bank details, credit card details and information about meals ordered for flights.[9] In Rizer's analysis on the introduction of the Act, he states US citizens accepted the requirement for tighter controls. He makes the point that US citizens' right to privacy and freedom to move throughout the US helped 'the enemy' to attack the World

[9] C. Kaunert, S. Leonard and A. McKenzie 'The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT', 21(4) *European Security* (2012), 474-496, p.483.

Trade Centre and the Pentagon.[10] It was not just the US that required tighter controls on air travel, in 2003 the UK introduced the e-Border scheme where, following a pilot programme that ran from 2004 to 2006, an intelligence led approach to border controls was introduced.[11] Under the pilot programme, from October 2005 this included processing PNR data on carefully selected routes.[12] Through the use of PNR data, the e-Borders scheme developed to identify and track movements of terrorists and national security targets as well as identify individuals for a range of criminal offences. It was found the intelligence supplied via e-Borders to the UK police, National Crime Agency and security services was regarded as an important component in the overall intelligence picture relating to the fight against terrorism and serious organised crime.[13] Although e-Borders has been replaced in the UK by 'The Border Systems Portfolio', PNR data is still perceived as an essential component in the range of programmes related to security and law enforcement and is expected to expand to ferry and train companies.[14] Other states have also introduced security control measures using PNR data. The Australian Department of Immigration and Border Protection is responsible for undertaking the risk assessment and clearance of all passengers arriving into and departing Australia. As part of its intelligence led approach to Australia's border protection, under section 64AF Customs Act 1901, the Department is authorised to access PNR data from all

[10] A. Rizer 'Dog Fight: Did the International Battle over Airline Passenger Name records Enable the Christmas day Bomber?' 60(1) Catholic University Law Review (2010), 77-105, p.83.
[11] House of Commons Committee of Public Accounts, 'e-Borders and successor programmes Twenty-seventh Report of Session 2015-16' HC 643, 4th March 2016,<http://www.publications.parliament.uk/pa/cm201516/cmselect/cmpubacc/643/643.pdf>.
[12] House of Lords European Union Committee (2008) 'The Passenger Name Record (PNR) Framework Decision: Report with Evidence' HL Paper 106, p.22.
[13] J. Vine CBE QPM, Independent Chief Inspector of Borders and Immigration 'Exporting the border? An inspection of e-borders, October 2012 – March 2013' <http://icinspector.independent.gov.uk/wpcontent/uploads/2013/10/An-Inspection-of-eborders.pdf>, p.3.
[14] G. Vina, 'UK spending watchdog criticises failure over e-borders programme' 3rd December 2015, Financial Times, <http://www.ft.com/cms/s/0/ed156742-990f-11e5-95c7-d47aa298f769.html#axzz4J0EfCJl5> 27th August 2016.

international air service operators flying to and from Australia.[15] In Canada since 2005 the Canadian Border Services Agency has collected PNR data under section 107.1, Customs Act 1985 with data protection of passengers' information provided under the Protection of Passenger Information Regulations 2005. In December 2001 British born Richard Reid (also known as the 'shoe bomber') attempted to blow up an American Airlines flight from Paris to Miami by detonating explosives hidden his shoe[16] and on the 25th December 2009 Umar Mutallab attempted to detonate explosives hidden in his underwear on a Northwest Airlines flight to Denver.[17] It appears the use of aircraft in terrorist attacks has galvanised a number of states to demand PNR data be made accessible regarding all flights to and departing from that state. Due to strict EU law on data protection, this demand for PNR data by non-EU states has been problematic, if not fractious at times, when negotiating agreements with the EU.

3. PNR Transfer Agreements with the US

In May 2004 an agreement was made between the EU Commission and the US Department of Homeland Security to transfer PNR data from Europe to the US.[18] An obstacle for the EU in agreeing to the US requests for PNR data centred on the EU's obligation that the EU should not transfer data to another country that cannot ensure a guarantee to provide an adequate level of protection.[19] Under the 1995 Data Protection Directive, prior to any data exchange it is the Commission's responsibility to asses if the third country has an adequate level of protection of basic freedoms and rights of individuals.[20] If the Commission finds the

[15] Australian Government Department of Immigration and Border Protection 'Purpsoe of collection and use of PNR data',https://www.border.gov.au/Trav/Ente/Goin/passenger-cards/collection-of-passenger-name-records, 29th August 2016.
[16] BBC news (2002) 'Shoe bomber pleads guilty' 4th October 2002 < http://news.bbc.co.uk/1/hi/world/americas/2298031.stm> 20th August 2016.
[17] Rizer, *supra* note 14, p.78.
[18] J. Argomaniz 'When the EU in the 'Norm-taker': the Passenger Name records Agreement and the EU's Internalisation of US Border Security Norms', 31(1) *Journal of European Integration* (2009), 119-136,p.123.
[19] Article 25(4) Data protection Directive 95/46/EC, Kaunert et al *supra* note 13, p.484, Argomaniz *supra* note 14, p.123.
[20] Article 25(3) Directive 95/46/EC.

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. 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[21] that could cost as much as USD 6,000 per passenger.[22]

Applying the1995 Data Protection Directive provisions, in 2006 the CJEU annulled the 2004 Decision.[23] Although the Court had the opportunity to deliberate on issues specifically related to the protection of personal data, the CJEU eschewed this as the main focus in their decision related to a consideration as to whether the Directive's scope in processing personal data fell outside Community law.[24] 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. The CJEU did add as the processing of PNR data was regarded as being necessary for safeguarding public security and for law enforcement purposes, this resulted in the agreement being annulled. In reaching this decision the Court referred to the earlier CJEU decision in *Lindqvist* 2003,[25] and in doing so applied the provisions of article 3(2) of the 1995 Directive that states the Directive does not apply to the processing of personal data in operations related to public security, defence, state security and areas of criminal law.[26] As a result, the CJEU held the processing of PNR data by private companies falls outside the scope of the 1995 Directive. Key to this decision was that the 2004 agreement was incorrectly based on EU transport policy (which was the first pillar of

[21] Kaunert et al, *supra* note 13, p.484.
[22] P. Pawlak 'Made in the USA? The Influence of the US on the EU's Data Protection Regime CEPS – Liberty and Security in Europe', Centre for European Policy Studies website (2009) <http://aei.pitt.edu/15102/1/made-usa-influence-us-eus-data-protection-regime.pdf>7th March 2016, p.4.
[23] *European Parliament v European Council and Commission* Joined cases C-317/04 and C-138/04.
[24] Ibid, para. 54.
[25] Case C-101/01.
[26] *European Parliament v European Council and Commission*, *supra* note 18, paragraph 59.

the EU under the Treaty of Union) rather than the third pillar (which was justice and home affairs). By adopting this position, an early opportunity by the CJEU was missed in addressing the sufficiency of personal data protection guaranteed by US authorities.[27] 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,[28] which, in turn, was replaced with a third PNR agreement between the EU and the US in 2012. In reaching the 2012 agreement, the EU Council announced the agreement's goal was by setting a legal framework for the transfer of PNR data it would assist in the prevention, detection, investigation and prosecution of terrorist offences and related crimes, as well as to help with serious cross-border crimes.[29]

3.1. Criticism of Previous EU PNR Agreements

The main criticism of early EU PNR data agreements 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.[30] To some observers this has been more prevalent in the EU-US agreements than in EU negotiations with other third countries.[31] In building its network of allies the EU's key partner has been the US. In spite of the divergent strategic cultures, judicial and data protection practices between the two, no other international actor has influenced previous EU policies more comprehensively than the US. This collaboration led to concerns about the impact it had on European citizens' privacy rights.[32] To provide an

[27] Kaunert et al, *supra* note 13, p.485.
[28] Ibid, p.485-486.
[29] Council of the European Union 'Council adopts new EU-US agreement on passenger Name Records (PNR)' 9186/12, PRESSE 173, (2012) <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf>, 4th March 2016.
[30] E. Ilbiz, C. Kaunert and D. Anagnostakis (2015) 'The counterterrorism agreements of Europol with third countries: data protection and power asymmetry', *Terrorism and Political Violence* DOI:10.1080/09546553.1092438, 1-18, p.2.
[31] Ibid, pp.8-13.
[32] J. Argomaniz, *The EU and Counter-Terrorism: Politics, polity and policies after 9/11* (Routledge, London, 2012), p.95.

understanding why this is the case Lehrke and Schomaker developed the network hypothesis. They state 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.[33] In applying this hypothesis Lehrke and Schomaker state by having a presence in many different EU venues, the US was able to exercise influence on the Council and Commission.[34] This builds on Pawlak's earlier study who states 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 US dictating and shaping the EU's security agenda.[35] Following the horrific Al Qaeda 9/11 attacks, the 2004 Madrid bombing and 2005 London bombings, one problem for the EU was by being in their infancy, the Justice and Home Affairs Commission along with its associated agencies Europol and Eurojust, were still developing. As a result they had little influence on the international stage either politically or on legal issues related to operational matters. An example of this was prior to the 2009 Treaty of Lisbon Europol had to sell to EU Member States projects that had to be given priority, whereas today projects developed with Member States must be in line with Europol's overall strategy.[36] With the EU realising the need to support international co-operation to counter the international terrorist threat, one can see how the US took advantage of the EU's relative unpreparedness to counter those threats. The impact of the Treaty of Lisbon provisions and the development of the EU's justice and home affairs agencies has changed significantly since the early years of the 21st century.

4. Legislative Proposals Prior to 2016 Directive

[33] J.P. Lehrke and R. Schmaker (2014) 'Mechanisms of Convergence in Domestic Counterterrorism Regulations: American Influence, Domestic Networks and International Networks', 37(8) *Studies in Conflict & Terrorism*, 689-712, p.693.
[34] Ibid, p.698.
[35] Pawlak *supra* note 17, pp.9-10.
[36] M. Busuioc, and M. Groenleer (2013) 'Beyond Design: The Evolution of Europol and Eurojust', 14(3) *Perspectives of European Politics and Society*, 285-304, p.293.

In relation to EU legislation covering passenger details in 2004 the Council adopted Directive 2004/82/EC on the obligation of carriers to communicate passenger data. The Directive concerned the transfer of advanced passenger information (API). API differs from PNR data as it covers the machine-readable zone on a person's passport that includes the passenger's name, date of birth, nationality and passport number.[37] The adoption of this Directive was relatively rapid as transferring API is less controversial than transferring PNR data. PNR data depends on information the passenger submits during the time of the reservation that includes more detailed personal information such as method of payment, dietary requirements, personal contact information and complete travel itinerary. By offering such detailed information the main concern advocates of data protection have is PNR data could be used for more detailed profiling by officers in relevant agencies on the background of individuals and the possible relationship to other persons being searched at port and border controls.[38] Data protection has been a major hurdle proponents of the need for legislative provisions related to PNR data acquisition and transfer had to overcome. Due to the EU's strict legislative provisions through the likes of the 1995 Data Directive and concern over privacy rights, it has been problematic in finding an effective solution that balances data protection requirements alongside protecting the security of states and its citizens.

Following the failed car bomb attacks in London and Glasgow Airport in June 2007,[39] the Commission introduced a proposal for a Framework Decision on PNR data with the aim of the Framework Decision to aid the prevention and combatting of terrorism and organised crime.[40]As only the UK, France and Denmark had primary legislation to capture PNR data,[41]

[37] M. Tzanou (2015) 'The war Against Terror and Transatlantic information Sharing: Spillovers of Privacy or Spillovers of Security?, 31(80) Utrecht Journal of international and European law, 87-103, p.96.
[38] E. Brouwer (2009) 'The EU Passenger name record System and Human Rights: Transferring passenger data or passenger freedom' CEPS Working Document no.320/September 2009, p.3.
[39] Argomaniz *supra* note 18, p.130.
[40] Tzanou *supra* note 37, p.95.
[41] Brouwer *supra* note385, p.4.

the aim of the Framework Decision was to provide harmonisation throughout the EU of PNR data collection and exchange ensuring safeguards are given to persons aimed at protecting their right to privacy.[42] As the Framework Decision contained a dearth of data protection provisions along with the PNR data to be transmitted virtually identical to the categories listed in the then EU-US Agreement,[43] it is understandable why there were concerned responses to the proposal. The proposal contained only two articles regarding the protection of personal data that were vague and lightweight in providing detailed, adequate data protection,[44] with no reference of consideration or adherence to the likes of the 1995 Data protection Directive. Although the proposal stated Member States had to set up Passenger Information Units (PIU) to be responsible for collecting and analysing PNR data, apart from stating any personal data collected revealing very personal information such as racial or ethnic origin, political opinions, religious beliefs,[45] there were no provisions related to how and when PIU's should protect personal data.

Referring to them as 'so-called- PIU's', in Brouwer's analysis of their role she could not see the setting up of a PIU as a better policy option to protect personal data.[46] Equally critical of the role of the PIU in the Framework Decision was the European Data Protection Supervisor (EDPS) who could not agree that a PIU would provide sufficient safeguards saying that additional provisions should be integrated to specify strictly the competences and legal obligations of PIU's.[47] Seeing the role of PNR data not being simply to identify a person, but contributing to carrying out risk assessments of person to obtain intelligence and make

[42] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes COM(2007) 654 final, Explanatory Memorandum, p.6.
[43] Tzanou *supra* note 37, p.96.
[44] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes COM(2007) 654 final, s*upra* note 42, articles 11 and 12.
[45] Ibid, article 3.
[46] Brouwer *supra* note 38, p.5.
[47] Opinion of the European Data Protection Supervisor on the draft Proposal for Council Framework Decision on the use of Passenger name record (PNR) data for law enforcement purposes (2008/C 110/01), paragraph 73.

associations between known and unknown people,[48] his most scathing opinions on the Framework Decision were in relation to necessity and proportionality issues. Regarding necessity, he deplored the lack of precise facts and figures related to the PNR saying:

> 'Numerous arrests' are reported with regard to "various crimes" in the UK … without precision as to the link with terrorism or organised crime. No details are given with regard to the US programme, except that 'the EU has been able to assess the value of PNR data and to realise its potential for enforcement purposes'[49]

The EDPS saw PNR data no more than a data mining tool and as such the risk presented to individuals must be clearly established.[50] Having similar views in relation to proportionality, the EDPS stated there needed to be a more in-depth and comprehensive analysis compared to what was presented in the Framework Decision proposal.[51] He saw the shortcomings contained in the proposals leading to a move towards a total surveillance society.[52] Equally critical of the Framework Decision proposal was Argomaniz who states that modelling the proposal on the US PNR scheme was carried out under the principle of reciprocity on information exchange with US authorities,[53] but is one where there is a reciprocity deficit on the EU side.[54] He argues that at this time not only did the EU-US PNR agreements demonstrate the asymmetrical relationship between the EU and the US, but also the likes of the 2007 PNR data Framework Decision proposal was an example of the US applying political and economic coercion to ensure European compliance. This may have been valid in 2009 when Argomaniz raised this point, but, as this article will demonstrate, due to developments in the EU, by 2016 this position has changed. There is currently at the very least a symmetrical relationship between the EU and US, if not one that is now asymmetrical in favour of the EU.

[48] Ibid, para. 14.
[49] Ibid, para. 27.
[50] Ibid, para. 29.
[51] Ibid, para. 34.
[52] Ibid, para. 35.
[53] Argomaniz supra note 18, p.131.
[54] Ibid, p.126.

Despite the lack of data protection provisions that would meet the EU standard, along with the damning criticism it resulted in the Framework Decision not being adopted,[55] in 2011 the Commission produced a proposal for a PNR Data Directive.[56] While there was a more detailed provision related to data protection,[57] with provisions related to the role of PIU's very similar to that in the 2007 Framework decision proposal.[58] The main concern with the 2011 PNR data Directive was the lack of protection of personal data, especially in relation to the transfer of PNR data to third countries. In an attempt to address this the following safeguards were contained in the Directive. Again one was an obligation placed on Member States to set up a PUI. The role of the PIU being to act as a filter by being responsible for collecting PNR data from air carriers, storing the information, analysing it and transmitting the analysis results to authorities competent in the prevention, detection, investigation or protection from terrorist offences or serious crime.[59] While it was proposed that Member States could transfer PNR data to third countries, it could only do so when the transfer was necessary in relation to terrorist offences and serious crime.[60] To ensure personal data was protected, the 2011 proposal stated that all procedures contained in the Directive could only be carried out under the conditions laid down under article 17-20 in the Framework Decision on the protection of personal data in police and judicial co-operation in criminal matters.[61] Although this Framework Decision will be repealed in May 2018 by Directive 2016/680,[62] under the Framework Decision[63] the data subject has the right to expect the competent authority to fulfil its duties,[64] which includes the right for the data subject to have a judicial

[55] Tzanou *supra* note 37, p.99.
[56] Directive 2011/0023.
[57] Ibid, article 11.
[58] Ibid, article 3.
[59] Directive 2011/0023, article 3.
[60] Ibid, article 1(2).
[61] Ibid, article 11.
[62] Directive 2016/608, para. 98.
[63] FD 2008/977/JHA..
[64] FD 2008/997/JHA, article 18.

remedy for any breach of the rights guaranteed to them by the applicable national law.[65] Where PNR data is transferred to a third country, prior to transferring the data there is a responsibility on the EU to ensure the third country has an adequate level of protection of the intended data processing.[66] Despite the European Commission's claim that the 2011 proposal had been subject to an in-depth scrutiny to ensure its provisions were compatible with fundamental rights, in particular article 8 of the EU's Charter of Fundamental Rights and Freedoms (CFRF) on data protection, the safeguards were deemed as insufficient in protecting personal data. The European Parliament expressed concerns regarding the proposed method of automatically processing PNR data using fact based pre-determined assessment criteria, saying they were very wide and thought such an assessment should never result in, '…profiling on the basis of sensitive data.'[67] Seeing insufficient protection of the individual's data privacy in the Directive, the EDPS questioned if the PNR data Directive provisions met the legal criteria of necessity and proportionality. In the format the 2011 Directive was presented, he did not perceive it as an effective tool in investigating terrorism and serious crime, rather he saw the move towards accessing and transferring PNR data doing nothing more but contributing towards a surveillance society.[68]

5. Concerns over the Surveillance Society: The 2013 Snowden Revelations

As the EDPS had concerns in 2011 that the PNR Data Directive was a move contributing towards the expansion of a surveillance society, such fears were confirmed two years later with the Snowden revelations. In 2013 Snowden passed on files and information regarding the practices of the US' National Security Agency (NSA) and the UK's General Communications Headquarters (GCHQ) intelligence agencies in relation to Operation

[65] FD 2008/997/JHA, article 20.
[66] FD 2008/997/JHA, article 14.
[67] European Commission *supra* note 3, p.10.
[68] Ibid, p.10.

PRISM to the journalist, Glen Greenwald who works for the UK newspaper, *The Guardian*.[69] In June 2013 both the *The Guardian* and *The Washington Post* broke with the news story regarding the NSA and the PRISM programme that gave US Federal agencies direct access to servers in the biggest web firms including Google, Microsoft, Facebook, Yahoo, Skype and Apple.[70] These top secret documents revealed the NSA was collecting telephone records of millions of US customers under a top secret order issued in April 2013 saying that, '…the communication records of millions of US citizens are being collected indiscriminately and in bulk regardless of whether they are suspected of any wrongdoing'.[71] The documents Snowden passed on revealed, it was not just US citizens subject to NSA surveillance, working alongside its UK counterpart GCHQ, the NSA gained access to the network of cables carrying the world's phone calls and Internet traffic. This allowed the NSA and GCHQ to process vast streams of sensitive personal information.[72] The co-operation between the UK and the US was not just limited to the NSA and GCHQ sharing information. It was revealed that through the access it had to the NSA's PRISM programme, from May 2012 to April 2013 GCHQ passed onto the UK's security agencies, MI5, MI6 and Special Branch's Counter-Terrorism Unit 197 PRISM intelligence reports [73]

The shock waves of the NSA's actions reverberated around the world, more so when it was revealed that politicians in the EU Member States were also spied on by the NSA, in

[69] G. Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian*, 6th June 2013, <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>, 1st September 2013.
[70] BBC News 'Web Privacy – outsourced to the US and China?' 7th June 2013 <http://www.bbc.co.uk/news/technology-22811002>, 1st September 2013.
[71] Greenwald, *supra* note 70.
[72] E. MacAskell, J. Borger, N. Davies, N. and J, Ball, 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21st June 2013 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, 1st September 2013.
[73] H. Hopkins, 'UK gathering secret intelligence via covert NSA operation', *The Guardian*, 7th June 2013, <http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>, 1st September 2013.

particular the German Chancellor Angela Merkel.[74] This resulted in a political dialogue between the EU and the US where the difference in legal culture between the two raised its head regarding individuals' rights, with the EU's focus being the dignity of citizens. In protecting fundamental human rights under the aegis of the rule of law, the EU requires a system of protection of an individual citizen's data privacy,[75] these are enshrined in a number of EU legal instruments. Conversely, no such explicit protection to a general right to privacy exists under the US Bill of Rights, it is inferred in the First, Fourth, Fifth and Ninth Amendments.[76] This difference in legal protection is important as Snowden's revelations had the potential to damage not only diplomatic relations between the US and EU Member States, it could have a detrimental long term affect in the terrorism intelligence and PNR data sharing between European counter-terrorism agencies and US federal agencies.

6. Criteria of Fitness for Purpose for a PNR Data Directive

From both the EU's PNR Agreements and the legislative proposals, one major stumbling block faced by the Council and the Commission in ensuring they meet the strict criteria in EU law related to data protection. There are more EU legal provisions related to data protection than just the 1995 Data protection Directive (although it underpins virtually all actions related to data protection). In addition to meeting this criteria, a PNR data Directive must be sufficiently robust to scrutiny by the CJEU. This section outlines those provisions and examines two important CJEU decision (*Digital Rights*[77]and *Schrems* [78]) related to data protection that lays down the threshold that must be met.

[74] G. Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, (Metropolitan Books: New York, 2014), p.141.
[75] C.C. Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing, Oxford, 2012), p.149.
[76] J. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113(1), *Yale Law Journal* (2004), 1011-1221,, p.1155.
[77] *Digital Rights* [2014]EUECJ C-293/12, [2014] 3 WLR 1607.
[78] *Schrems v Data Protection Commissioner* [2015] EUECJ C-361/14.

6.1. EU Data Protection Laws

In relation to data protection article 16 of the Treaty on the Functioning of the EU (TFEU), states everyone has the right to the protection of personal data concerning them. Under article 16 TFEU the European Parliament and the Council must act in accordance with ordinary legislative procedure, laying down rules protecting the processing of personal data by Union institutions, bodies, office and agencies when carrying out activities that fall within the scope of EU law. This legal obligation is also present in article 39 in the Treaty of Union. Underpinning these articles' provisions is the EU's CFRF. Since the Treaty of Lisbon 2009 came into force, the CFRF has become a legally binding document ensuring all EU institutions and Member States apply the Charter's principles when implementing EU law. Article 8 CFRF states that everyone has the right to the protection of personal data concerning them. When EU institutions or Member States access the data it, '…must be processed fairly for specified purposes on the basis of consent of the person concerned or some other legitimate basis laid down by law.'[79] This is in addition to the respect they must have for a person's right to their private and family life, home and communication.[80]

The 1995 Data Protection Directive[81] states personal data can only be collected for specified, explicit and legitimate purpose and must not be processed in a way incompatible with these purposes.[82] Member States can only derogate from the 1995 Directive where it is necessary to safeguard national security, defence, public security and the prevention, investigation, detection or prosecution of criminal offences.[83] The Directive on the protection of personal data processed for the purposes of preventing, investigating, detecting or prosecuting criminal

[79] Article 8(2) CFRF.
[80] Article 7 CFRF.
[81] European Parliament and Council Directive 95/46/EC.
[82] Ibid, article 6(1)(b).
[83] Ibid, article 13(1).

matters[84] came into force 5thMay 2016 for Member States to transpose into their national law by 6th May 2018.[85] In the preamble it is recognised that rapid technological developments and globalisation has brought new challenges for the protection of personal data where the scale of collecting and sharing this data has increased significantly and this includes by agencies involved in the prevention, investigation or detection of criminal offences.[86] The Directive states that in the processing of personal data these agencies can only collect it for specific, explicit and legitimate purposes[87] and to be lawful, the processing of personal data has to be necessary in the prevention, investigation or detection of criminal offences.[88] The Directive is also very clear that when processing personal data fundamental rights and freedoms must be protected, especially the right of the protection of personal data.[89] Important in protecting personal data are the safeguards present in any legislative provision, and drawing out from the Directive that are pertinent to the 2016 PNR data Directive this includes:

1. Member States and the EU itself shall crate a 'controller'[90] who have a number of obligations under the Directive to oversee the processing and exchange of personal data. This includes ensuring the requests by relevant agencies for personal data are proportionate to the purposes of processing the data,[91] and integrating the necessary safeguards in to the processing of the data;[92]
2. Member States shall provide a data protection officer[93]whose roles include advising the controller and employees from agencies carrying out the processing of personal data and monitoring compliance with the Directive;[94]
3. Where the data subject conspires their personal protection rights have been infringed, Member States must ensure data subjects have the right to an effective judicial remedy (which in practice will be through a judicial review process).[95]

[84] Directive 2016/680.
[85] European Commission (2016) Reform of EU data protection rules < http://ec.europa.eu/justice/data-protection/reform/index_en.htm>, 19th May 2016.
[86] Directive 2016/680, para. 2.
[87] Ibid, para. 29.
[88] Ibid, para. 35.
[89] Ibid, article 1(2).
[90] Ibid, article 3(8).
[91] Ibid, article 19.
[92] Ibid, article 20.
[93] Ibid, article 32.
[94] Ibid, article 34.
[95] Ibid, article 54.

One part that directly pertains to the 2016 PNR Data Directive in the 2016 protection of personal data Directive is the transfer of personal data to third countries or international organisation. In addition to the transfer of personal data to a third country having to meet the requirements of being necessary and proportionate for the purposes of preventing, investigating or detecting criminal offences,[96] it is of paramount importance that the third country with whom the data is transferred has an adequate level of protection of personal data.[97] If there is an absence of adequacy or protection in a third country, transfer of personal data under the 2016 Directive can only occur where such conditions are implemented under a negotiated legally binding instrument.[98]

6.2. The Impact the CJEU's Decisions in *Digital Rights* and *Schrems* on Data Protection

In *Digital Rights* the CJEU held Directive 2006/24/EC on the collection of bulk data by Member States' intelligence and policing agencies was invalid as it contravened EU data protection laws. The CJEU stated two important legal issues were required 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;
2. Minimum safeguards are imposed to provide sufficient guarantees effectively protecting personal data against the risk of abuse and against unlawful access and use.[99]

In elucidating this point, the CJEU stated data can only be retained when it was necessary and proportionate to do so, albeit subject to the provisions of EU law and in particular the European Convention on Human Rights (ECHR) as interpreted by the European Court of

[96] Ibid, article 35.
[97] Ibid, article 36(1).
[98] Ibid, article37..
[99] *Supra* note 11, para. 54.

Human Rights (ECtHR). Ojanen's analysis of *Digital Rights*, 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.[100]

The CJEU decision in *Digital Rights* was not a 'total knockout' to mandatory retention.[101] 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. By imposing on the EU legislator the responsibility to protect fundamental rights, *Digital Rights* imposes substantive instructions on law-makers at EU and Member States' level to guarantee the protection of data protection and, importantly, provides a strict judicial scrutiny test.[102]

In S*chrems*, since 2008 Maximillian Schrems, an Austrian citizen, used the social media network, Facebook. 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.[103] The Irish High Court refered the case to the CJEU.

---

[100] T. Ojanen, 'Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance', 10(3) *European Constitutional Law Review*, (2014), 528-541, p. 537.
[101] Ibid, p. 539.
[102] M. Granger and K. Irion, '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', 39(6) *European Law Review* (2014), 835-854, p.849.
[103] Ibid, paras. [26] – [30.]

In his opinion judgment, 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.[104] In this case under the US' 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.[105] The CJEU declared the 2000/520 Decision invalid[106] and consequently brought to an end an important EU-US trade agreement, the Safe Harbour Agreement. Crucial to the Court reaching this decision were the requirements of article 25 of the 1995 Data Protection Directive concerning 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.[107]

The most pertinent part of article 25 related to the issue in *Schrems* is the Commission's responsibility to find that the third country ensures an adequate level of protection of basic freedoms and rights of individuals.[108] 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.[109] 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,[110] Advocate General Bot said that the protection

[104] *Schrems supra* note 81, para. 210.
[105] Ibid, paras. 210 and 211.
[106] *Schrems supra* note 12, paragraph [107].
[107] art 25(2) Directive 95/46/EC.
[108] Ibid, art 25(6).
[109] Ibid, art 25(4).
[110] Schrems supra note 12, para. 73.

implemented by the third country may differ from EU law, but it must provide adequate protection that is equivalent to that afforded by the 1995 Directive.[111] 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.[112] 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[113] and it is expected the Commission will regularly review the third country's level of protection.[114] The CJEU 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.[115]

7. The 2016 PNR Directive

A new draft text on an EU system for processing PNR data was tabled by Member of the European Parliament (MEP) Timothy Kirkhope, which was discussed in the EU's civil liberties LIBE Committee on 26 February 2015.[116] The draft text's introduction covers issues discussed by MEP's, which includes 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*. The terrorist attacks in Paris in January and November 2015 may have accelerated movement by

[111] Ibid,, para. 141.
[112] Ibid, para. 142.
[113] Ibid, para. 147.
[114] Ibid, para. 137, *Schrems supra* note 12, para. 76.
[115] Ibid, para. 94.
[116] P. Bakowski and S. Voronova 'The proposed EU passenger name record (PNR) directive: Revived in the new security context, European Parliament Briefing' April 2015, <http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf >, 9th March 2016, p.4.

EU officials in introducing the 2015 PNR Directive proposal. 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 and the European Parliament in early 2016.[117] As a result, the PNR data Directive 2016/681 was introduced on the 27th April 2016 to enable the transfer of PNR data between Member States and third countries. Following the previous unsuccessful attempts to introduce PNR data legislation, key to this Directive being fit for purpose is in meeting the EU's data protection laws as well assisting in preventing acts of terrorism.

7.1 A comparison between 2011 and 2016 Directive

While the processing of the PNR data in the two Directives is on a case-by-case basis to deal with terrorism and serious crime, in comparison to the 2011 proposal, the 2016 Directive contains greater safeguards in relation to protecting personal data. While both PNR Data Directives state that Member States establish a PIU[118] with the responsibility to ensure data is processed correctly with consideration of protection of personal data,[119] the 2016 Directive goes further stating the PIU must appoint a data protection officer who will be responsible for implementing safeguards.[120] The PNR data storage is to be carried out exclusively by PIU's within a secure location within the territory of the Member State.[121] Not considered in the 2011 version, Member States shall ensure a data subject has the right to contact the data protection officer as a single point of contact on all issues related to the processing of the subject's PNR data.[122] In the 2016 Directive Europol is also entitled to request PNR data on a

[117] T. Papademetriou 'European Union: Draft Directive on Collection and Transfer of Air Passenger Record Data', 23rd December 2015, Library of Congress, retrieved from <http://www.loc.gov/law/foreign-news/article/european-union-draft-directive-on-collection-and-transfer-of-air-passenger-record-data/>, 9th March 2016.
[118] Directive 2016/681, article 4, Directive 2011/0023, article 3.
[119] Directive 2016/681, article 4(2)
[120] Ibid, article 5(1).
[121] Ibid, art. 6(8).
[122] Ibid, art. 5.

case-by-case basis where the request is strictly necessary to strengthen Member States in preventing, detecting or investigating specific terrorist offences or serious crime provided it is within Europol's competence. In such circumstances Europol must inform the data protection officer of each exchange.[123] This inclusion is significant as Europol's role has not only increased in supporting and assisting in police co-operation among Member States and third countries, post 2009 Treaty of Lisbon Europol's activities has come under the scrutiny of the European Parliament[124] and the CJEU via the judicial review process. Added to this, citizens in each Member State can apply for the judicial review process against the respective public bodies in either the domestic courts or the CJEU. This provides another safeguard in protecting personal data. Also contained in the 2016 Directive, which was not included in the 2011 version, is the requirement that Member States provide a national supervisory authority to verify the lawfulness of the data processing and deal with and investigate complaints (which includes informing complainants of the progress and outcome of the investigations).[125] The role of the supervisory authority is extensive in protecting citizens' rights.[126] The supervisory authority must be independent,[127] have qualifications, experience and skills in the area of personal data[128] and the appointment must be made by means of a transparent procedure.[129]

The 2016 PNR Data directive makes it very clear that transfer of PNR data to a third country can only be transferred by a Member State once it is has been ascertained the third country's use of the data is to make use of it in accordance with the Directive's aim and that country

[123] Ibid, art. 10.
[124] Treaty of Lisbon 2009, article 69G(2).
[125] Directive 2016/681, article 15.
[126] Directive 2016/680, article 46.
[127] Ibid, article 42.
[128] Ibid, article 43(2).
[129] Ibid, article 43(1).

has sufficient legal safeguards in place to protect that data.[130] In all cases where PNR data is transferred to a third country the Member State must inform the data protection officer.[131] Underpinning all of this is article 13 of the Directive that states each Member State shall provide that every passenger subject to PNR data has the protection of their personal data, rights of access, rectification, erasure and judicial redress as laid down in Framework Decision 2008/977/JHA regarding the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This will only apply to the 6th May 2018 when it is repealed by the 2016 Directive on protecting personal data in criminal matters.[132] In the 2016 Directive there has been an increase in the provision of legal safeguards protecting personal data that appears to meet the EU's legal requirements provided for in EU legal instruments and follows the guidance from the CJEU's decisions.

7.2 Assessing the 2016 Directive's Fitness for Purpose: Data Protection

Even though there have been extensive changes regarding the protection of personal data, there are still concerns with the 2016 Directive regarding it being fit for purpose. In 2015 the EDPS published his opinion on the current 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,[133] 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 passengers a year. The EDPS recommended that the Directive

[130] Directive 2016/681, art.11.
[131] Ibid, art. 11(4).
[132] Directive 2016/680, article 59, where articles 14-18 of the Directive will apply.
[133] 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' <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf>, 14th March 2016, p.15.

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.[134] 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.[135] This is questionable. In addition to terrorist activity, Annex II of the 2016 Directive lists specific criminal activity, all of which are serious crimes that are punishable by a custodial sentence for a maximum period of at least three years.[136] To meet the criteria contained in the 2016 Directive's safeguards, it is assumed that where it is not related to terrorist activity, an application for access to PNR data will specify one of those crimes for it to be granted. Surely this is sufficiently specific?

To help allay some of these concerns could be the role Europol plays. The EDPS makes a pertinent recommendation 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.[137] This is a logical step. As stated, Europol is subject of judicial scrutiny as post 2009 Treaty of Lisbon Europol's actions are subject to judicial review by the CJEU[138] and this would help ensure legal redress by citizens who are concerned their data was misused. The Treaty of Lisbon has not just ensured there is solely judicial scrutiny of its actions, the Treaty also affords the European Parliament and Member States' parliaments authority over Europol.[139] In addition to this Europol's role in counter-

[134] Ibid, p.7.
[135] Ibid, p.13.
[136] Directive 2016, article 3(9).
[137] EDPS opinion, *supra* note 133, p.13.
[138] Busuioc and Groenleer *supra* note 36, p.299.
[139] J.D. Ochipinti 'Still Moving Towards a European FBI? Re-Examining the Politics of EU Police Cooperation', 30(2), *Intelligence and National Security*, (2015), 234-258, p.246.

terrorism and in dealing with serious criminal activity has grown both within the EU and on the international stage. Helping this growth has been Europol's permanent unit of experts to provide national authorities with analysis and support. As a result 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.[140] 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.[141]

As Europol has the staff, resources and departments that are legally accountable, and, experienced in ensuring compliance with EU personal data law, a logical policy step would be for Member States to consult Europol to scrutinise requests for PNR data on a case-by-case basis, especially in cases of a third country request. With Europol scrutinising and co-ordinating PNR data transfer, it will ensure a greater degree of protection of EU citizens' personal data when sharing of the data with third countries.

7.3 Assessing the 2016 Directive's Fitness for Purpose: Preventing Terrorist Acts

In the five years since the 2011 PNR Data Directive failed to be introduced there has been a changing landscape of international terrorist activity, mainly through the rise and influence of

[140] Ibid, pp.239-241.
[141] Europol 'Europol's European Counter terrorism Centre Strengthens the EU's Response to Terror', 25th January 2016 <https://www.europol.europa.eu/content/ectc>, 4th March 2016

the terrorist group Islamic State (IS). There are two aspects to this, one being the number of EU citizens travelling from the EU to join IS in its self-proclaimed caliphate in Syria/Iraq and the terrorist attacks in Europe in 2015 and 2016 carried out by IS inspired terrorists. In addition to this a number of EU Member States have introduced anti-terrorism related legislation to deal with citizens travelling to conflict areas related to terrorist activity. The UK has granted powers for seizure of passports at ports and airports from persons suspected of involvement in terrorism[142] and Germany has made it a crime to travel outside the country with the intent to receive terrorist training.[143] Access to PNR data is very useful to assist investigations on individuals to assess if they are *bone fide* passengers or if they meet the provisions under this type of legislation. This is important as PNR data could reveal information on individuals who have not come to the attention of the competent authorities but who received assistance with those who have. As PNR data provides more details that API such as who booked the travel and how it was paid may just be sufficient to alert those authorities of either a potential terrorist threat on or in the vicinity of an aircraft, or of travel to a destination linked to other terrorist activity. This can also be applied to serious crime such as drug trafficking where members of an organised crime groups make the travel arrangements for drug mules.

Prevention of terrorist attacks or crime is notoriously difficult to measure. Since the introduction of PNR data exchange and the security measures at airports brought about by passenger attempts to use aircraft in acts of terrorism, there have been very few incidents since the 2009 attempt at Denver. The acquisition and exchange of PNR data has contributed in making it difficult for terrorists to use aircraft in acts of terrorism. As stated above, this is not the only activity to link terrorism and air travel. As air travel is still used by those directly

[142] s. 1 Counter-Terrorism and Security Act 2015.
[143] Gesetz zur Anderung de Verfolgung der Vorbereitung Schweren Staatsgefahrdenden Gewalttaten, 2015.

or indirectly associated with terrorist organisations PNR data is a very useful source of information to assist counter-terrorist investigators identifying patterns of behaviour or simply to target individuals for port stops such as those in the UK under Schedule 7 terrorism Act 2000. The value of this intelligence in preventing terrorist acts, thereby saving many innocent lives cannot be underestimated, and the same principle can be applied to those involved in investigating serious criminal activity.

7.4 Assessing the 2016's Directive's Fitness for Purpose: Robustness to Legal Challenges and does it go far Enough?

At the time of writing an important CJEU decision is pending in relation to the Canada-EU PNR agreement.[144] Following a referral by the European Parliament in November 2015 regarding concerns over protection of personal data in the EU-Canada PNR data agreement signed in 2014.[145] The case went to the CJEU in April 2016 where the European Parliament's concerns centred on period of time prior to anonymisation of PNR data, the necessity of processing PNR data in terrorist investigations, period of retention of PNR data and independent supervision of data protection in Canada.[146] On the 8th September 2016 the Advocate General's Opinion was published where Advocate General Mengozzi in finding some aspects of the agreement was compatible with the EU's CFRF, he also found certain provisions of the agreement were contrary to the EU's CFRF:

1. in particular provisions allowing PNR data being processed he saw as being beyond that being strictly necessary (terrorist offences and serious forms of transnational crime);
2. the provision for processing, use and retention by Canada of PNR data containing sensitive data;

[144] Case A-1.15.
[145] Council of the European Union 'Signature of the EU-0Canada agreement on Passenger Name Records (PNR)' 10940/14 PRESSE 339 < http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwjipderyJvPAhXIA8AKHYRCDQoQFggtMAM&url=http%3A%2F%2Fwww.consilium.europa.eu%2Fen%2Fpress%2Fpress-releases%2F2014%2F06%2Fpdf%2Fsignature-of-the-eu-canada-agreement-on-passenger-name-records-(pnr)%2F&usg=AFQjCNHy3-FwwFuavf4V171uBAEG2ITQ-A>.
[146] D. Naranjo (2016) 'CJEU hearing on the EU-Canada PNR agreement: Still shady' Protecting Digital freedom website < https://edri.org/cjeu-hearing-on-the-eu-canada-pnr-agreement-still-shady/>.

3. disclosure by Canada of information without a connection to public security as agreed;
4. retention of PNR data by Canada for up to five years
5. allowing PNR being transferred to Canada without satisfactory independent supervision that that data would not be transferred to by Canada to another foreign body.[147]

Many human rights groups celebrated this decision. In making links between the agreement and the 2016 Directive they see it as a probable death knell for the Directive. For example, the group 'accessnow' had the headline that the agreement 'won't fly', but even this group admit if sufficient safeguards were put in place, the agreement could be legal under EU law.[148] It is suggested that in linking the issues raised in the decision on the agreement to the Directive these groups' argument is premature, optimistic at best. The reason being, one that is the nub of the issue elucidated above, the 2016 Directive has been drafted to ensure it meets the strict EU law on data protection with a numerous safeguards in place to prevent abuse of personal data. While Advocate General's Decision A-1.15 may be the death knell for current separate EU PNR data agreements with third countries, it must surely be assumed the 2016 Directive will be the instrument used to underpin any future agreements to transfer PNR data to third countries.

Part of the problem could be the term 'PNR data', which for many MEP's has become increasingly a metaphor for surveillance of EU citizens by foreign states[149] that emanates from suspicions behind the earlier PNR agreements, especially with the US. This is seen in Huijboom and Bodea's study that led them to state MEP's have not only framed the PNR debate through the lens of EU citizens' rights, but also through the lens of the EU's

[147] Court of Justice of the European Union Press release No 89/16, 'Advocate General's Opinion in the Request for an Opinion 1/15', Luxembourg 8th September 2016 < http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160089en.pdf>.
[148] Accessnow (2016) 'Advocate General Opinion on EU Canada PNR agreement: it won't fly' 8th September 2016 < https://www.accessnow.org/advocate-general-opinion-eu-canada-pnr-agreement-wont-fly/>.
[149] N. Huijboom and G. Bodea, 'Understanding the political PNR Debate in Europe: A Discourse Analytical Perspective', 16(2), European Politics and Society, (2015), 241-255, p.248.

democratic deficit.[150] In attempting to understand why the majority of Europeans hold such narrow focus on the philosophy on data protection resulting in them having a high concern for and holding strict adherence to privacy rights, Rizer suggests it emanates from the death lists and domestic spying in both Nazi Germany and in Soviet-ruled Eastern Europe.[151] This fear seems to be reflected in both the political and legal research in this area. On the 2016 PNR data Directive, when it was still in its proposal stage Tzanou saw in the EU's fight against terrorism, privacy and data protection taking 'a back seat' to security initiatives.[152] This observation has validity when examining the early PNR agreements and PNR legislative proposals, but not so much with the 2016 Directive, which is replete with data protection safeguards. Influential in many studies on intelligence gathering, especially in relation to PNR data is Argomaniz's 2009 work where he correctly states at that time there was an asymmetrical relationship between the EU and the US, with the US having a more dominant relationship with the EU.[153] Seven years later that position has changed. As the EU's agencies have developed so has its law and the confidence of the CJEU to overturn international agreements. As seen in *Schrems*, if the CJEU see breaches of EU law, the Court is not averse to making decision that result in the ending of important and lucrative trade agreements with the US. As a result it now appears there is symmetrical relationship between the EU and the US. Even Tzanou concedes the point that being based on the rule of law that respects human rights the EU is seen as a leader of 'moral good'. Security interests and data protection are not exclusive entities, they are and should be intertwined, especially where security interests are concerned in protecting the most important human right, the right to life.

[150] Ibid, p.250.
[151] Rizer, *supra* note 10, p.82.
[152] Tzanou *supra* note 37, p.100.
[153] Argomaniz *supra* note 18, pp.126-127.

If there is one area where the 2016 Directive is deficient is it covers air travel only. As stated, the UK has had PNR data programmes in place since 2004 and the UK is currently looking to expand this to rail and ferry travel. When the PNR Framework Decision was introduced the UK's House of Lords European Union Committee saw the Framework Decision limited by only covering air travel. Their 2008 Report on the Framework Decision stated the UK government would like to extend PNR data to cover other forms of travel.[154] As PNR data acquisition and exchange has assisted in making air travel safer, as terrorists planning to carry out an attack on an aircraft know they can be traced and prevented from carrying out that attack, this seems to be a logical step. If PNR data was extended to include international train travel on mainland Europe and the Eurostar service between the UK and Paris/Brussels as well as international ferry services in Europe, this would increase the ability of policing agencies investigating terrorist acts and serious crime to monitor the movement and activities of suspects. This would not be just monitoring those who suspected of planning attacks on these forms of transport, but also monitor suspects' movements around Europe. Both the Paris and Brussels attacks in 2015 and 2016 involved terrorists that travelled around Europe and, accepting this will not prevent terrorists and criminals from using other forms of transport, it will result in making their travel more difficult with the correlative effect being making Europe safer. Seeing how for the last fourteen years it has been problematic in introducing PNR data legislation that focuses solely on air travel, this may be too early to take this step due to the fears of widening even further access to citizens' personal data. In itself this factor does not affect the 2016 Directive's fitness for purpose related to air travel.

8. Conclusion

[154] House of Lords European Union Committee, *supra* note 16, p.15.

In addition to the serious criminal activity ongoing with the EU, the current terrorist threat facing many EU Member States alone necessitates the importance in introducing the 2016 PNR Data Directive. In the past eighteen months 179 citizens have been killed with many more seriously injured in three separate terrorist incidents in EU Member States. It is unlikely the terrorist threat in Europe will abate in the coming years. One of the aims of the 2016 PNR Data Directive is to enhance the ability of agencies investigating terrorist activity in preventing terrorist attacks and to monitor air travel of persons suspected of being involved in terrorist activity. On the grounds of necessity, there is a need for a PNR data Directive. While it is important for the EU and its Member States to ensure the needs of national security are met, it is equally important fundamental rights and freedoms are also met. Neither is mutually exclusive. In relation to PNR data while it is important to protect personal data, it is equally important a balance is made between the two as protecting security equates to protecting citizens' right to life.

The lack of personal data protection has been the undoing of previous EU PNR data agreements and attempts by the EU to introduce legislation.. As EU law has developed in this area, it has incrementally tightened the protection of personal data. This is reflected in the CJEU decisions, none more so than in the *Digital Rights* and *Schrems* cases. *Digital Rights* laid down criteria EU law must adopt in its legal instruments related to the protection of personal data in criminal matters. While the 2016 Directive on protecting personal data in criminal matters evolved due to concerns with the increase of the surveillance society, one can see the influence of the CJEU in *Digital Rights* in the drafting of this Directive. Equally important has been the CJEU's decision in *Schrems* which ended an EU-US trade agreements on the ground's the US had an inadequate provisions for the protection of personal data. This has had an important bearing on the transferring of data from EU Member States to third countries in all aspects of EU activity, including terrorism and criminal activity. These

developments have contributed to there being a more symmetrical relationship between the EU and the US.

Returning to the 2016 PNR Data Directive, there are a number of safeguards in place to ensure personal data is protected. This ranges the creation and responsibilities of the PIU and the data protection officers in each Member State, to the ability of citizens to have judicial supervision. All of these provisions are underpinned by the protection of personal data as laid down in the Framework Decision 2008/977/JHA, to be replaced in 2018 by the more all-encompassing 2016 Directive on the protection of personal data in criminal matters. In addition to the safeguards, the 2016 Directive is sufficiently specific and proportionate as it only applies to specific serious crimes and terrorist incidents. The Directive not only has sufficient safeguards, it ensures the data is accessed and transferred where necessary with sufficient specificity to meet EU law requirements. In addressing if the 2016 PNR Data Directive is fit for purpose, it is argued in relation the points made above it is.