EU-US Counter-Terrorism Agreements for Tracking Money and Airline Passengers: A Challenge to Right to Privacy and Personal Data Protection

Elif Mendos Kuşkonmaz*

Abstract

This article examines the lawfulness of the EU-US Terrorist Finance Tracking and Passenger Name Records Agreements which provide for the transfer of EU-originated data to US law enforcement authorities for countering terrorism, from the perspective of EU fundamental rights. It considers the historical background and scope of each agreement in separate and then proceeds to analyse whether or not the transfer of EU-originated data to the US under these agreements is necessary and proportionate, taking account of the counter-terrorism interests on one hand and rights and civil liberties of EU citizens on the other. The central discussion will revolve around the compatibility of both agreements with the safeguards of the fundamental rights as laid down under the EU Charter of Fundamental Rights in general and of the right to respect for privacy and to personal data protection in particular.

Keywords

Right to Privacy – Personal Data Protection – Personal Data Transfer – Financial Data – PNR data – Proportionality Principle – EU-US Terrorist Finance Tracking Agreement – Passenger Name Records Agreements – Counter-Terrorism.

1. Introduction

The revelations made in June 2013 by Edward Snowden surrounding the United States (US) surveillance systems confirmed what privacy advocates have been talking about for a long time: the existence of a US government programme of a systematic and disproportionate retention of data about, including but not limited to, all European citizens.[1] During the turmoil caused by these revelations, the Court of Justice of the European Union (CJEU) declared the Data Retention Directive 2006/24 invalid in the case of *Digital Rights Ireland*.[2] Thereby, the Court affirmed the growing importance of the Charter of Fundamental Human Rights of

* Ph.D. student at Queen Mary, University of London., e.m.kuskonmaz@qmul.ac.uk. The author is indebted to Prof Elspeth Guild for her valuable comments on this article. The author also wishes thank the reviewers for their valuable suggestions.

[1] See generally, Didier Bigo et al, 'Mass Surveillance of Personal Data by EU Member States and its compatibility with EU law', CEPS Paper in Liberty and Security in Europe, No 62 (CEPS November 2013).

[2] Joined Cases C293/12 and C594/12 *Digital Rights Ireland v. The Minister for Communications, Marine and Natural Resources and Other*s EU:C:2014:238 [2013].

the European Union (Charter) as a tool to counter privacy-intrusive measures which weaken the fundamental rights of European citizens.

These pivotal incidents fostered discussions on the lawfulness of the Terrorist Finance Tracking Program Agreement and EU-US Passenger Name Records Agreement. The former provides for the transfer of EU-originated financial data to the United States and is aimed at fighting against terrorism and its financing. The latter focuses on the mobility of people and regulates the Passenger Name Records transfer by European airline companies to the US law enforcement authorities for the prevention and investigation of terrorism and certain transnational crimes as specified under the Agreement. Evidently, both agreements rely on countering terrorism as the objective to justify the systematic collection and storage of personal data.

Having said that, taking a deeper look at both agreements, at least from a European Union (EU) perspective, would raise the question of whether the retention and subsequent transfer of data about all individuals, regardless of their past or present criminal background, for the purpose of countering terrorism is consistent with EU citizens' right to privacy and data protection. In particular, given the impact of the June 2013 revelations and the CJEU's decision on the Data Retention Directive, questions as to the lawfulness of such data sharing measures still linger. Do these agreements respect fundamental rights and balance them against public security? This article seeks to analyse the lawfulness of the Terrorist Finance Tracking Program and Passenger Name Records Agreements from an EU fundamental rights perspective. The emphasis will be placed upon whether it is necessary and proportionate to allow such data transfers required by both agreements, taking into account the aim of countering terrorism on one hand and fundamental rights of EU citizens on the other. The central discussion in respect of breaches of fundamental rights of individuals will be based on the right to privacy and personal data protection, as safeguarded by the Charter. This paper will argue that both agreements fall short of respecting EU citizens' right to privacy and personal data protection. Therefore, they need to be reconsidered in line with the ongoing importance of the fundamental rights at least at the EU level.

To support this argument, this article will map the negotiations leading to the Terrorist Finance Tracking Program Agreement and Passenger Name Records Agreement separately. Having framed the current scope of both of the agreements, it will examine whether they are compatible with the right to privacy and personal data protection as guaranteed under the Charter.

2. Terrorist Finance Tracking Program Agreement

From the very beginning of its negotiations until today, and more importantly in the aftermath of the revelations made in June 2013 by Edward Snowden on the US surveillance programs[3], the Terrorist Finance Tracking Program Agreement (TFTP) has been one of the most controversial agreements in the context of international cooperation on countering terrorism.[4] The crux of the controversies is whether or not countering terrorism can be

[3] For the European Parliament's response to the US NSA surveillance systems see; European Parliament, Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental right and on transatlantic cooperation in Justice and Home Affairs, A7-0139/2014, (21 February 2014).

[4] For the Members of the European Parliament's call for suspending the TFTP Agreement see; European Parliament Resolution on the suspension of the TFTP agreement as a result of US National Security Agency surveillance, P7_TA (2013)0449, (23 October 2013). For European Commission's rejection for such suspension see; European Commission, 'The EU-US TFTP Agreement: main elements', MEMO/13/1060, (27 November 2013). See also; Dutch Data Protection Authority, 'Data protection authorities have not found any violations at SWIFT', (08 May 2014) Press Release,

considered as a robust legal ground for the infringement of the right to privacy and protection of personal data. Before further discussing this issue, this part of the article explores the key events towards the conclusion of the TFTP agreement. Later, it analyses how financial data transfer operates under the Agreement. Finally, it gives a general overview of the proposed system for tracking terrorist finance at a European level.

A. The Media Disclosure of the Terrorist Finance Tracking Program

The pathway towards an agreement on the transfer of the EU-originated financial messaging data to the US Department of the Treasury (UST) started when the existence of a program called Terrorist Finance Tracking Program (US TFTP) was unveiled by The New York Times journalists in June 2006.[5] According to this media disclosure, the program was initiated by the US administration in the aftermath of the September 2001 attacks and US authorities were able to gain access to financial messaging data held in the Society for Worldwide Interbank Financial Telecommunications' (SWIFT) database under this program.[6] SWIFT is a Belgian based company which undertakes the vast majority of electronic financial transactions for financial institutions around the world.[7] The US TFTP is still in effect today and its goal is to carry out terrorism investigations by way of tracking terrorist money flows.[8] The program is based on administrative subpoenas in which transfer of financial records for terrorism investigations are required.[9] Shortly after the initiation of the US TFTP, SWIFT was subjected to these administrative subpoenas simply because by that time SWIFT had database storage in the US and therefore it had to comply with those subpoenas.[10] This program triggered an outrage at the international level, mostly from the EU, in which privacy protections are more stringent than in the US.[11]

The UST requests made to SWIFT under the US TFTP consisted of information regarding data transfers from the EU to third countries and thus these transfers had to be compatible with both the EU's and Member States' national data protection legislation, which require a judicial authorisation to allow such data transfers.[12] Any derogation from this authorisation principle had to be proportional and found either in law or in an international agreement.[13] Nevertheless, the US TFTP was neither an EU law nor international agreement

---

<https://autoriteitpersoonsgegevens.nl/en/news/data-protection-authorities-have-not-found-any-violations-swift> (accessed on 26 April 2016).

[5] Eric Lichtblau and James Risen, 'Bank Data Is Sifted by US in Secret to Block Terror' New York Times (Washington, 23 June 2006) <http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=1&_r=0> (accessed on 26 April 2016).

[6] ibid.

[7] For more information on SWIFT see; <http://www.swift.com/index.page?lang=en>.

[8] The US Department of the Treasury, 'TFTP Fact Sheet', <http://www.treasury.gov/resource-center/terrorist-ilicit-finance/Terrorist-Finance-Tracking/Documents/TFTP%20Fact%20Sheet%20revised%20-%20(8-8-11).pdf> (accessed on 26 April 2016).

[9] Patrick Connorton, 'Tracking Terrorist Finance through SWIFT: When US Subpoenas and Foreign Privacy Law collide' (2007) 76 Fordham L Rev 283, 288.

[10] ibid. European Parliament, 'SWIFT Statement by Francis Vanbever - Chief Financial Officer, Member of the Executive Committee' (04 October 2006) Hearing <http://www.europarl.europa.eu/hearings/20061004/libe/vanbever_en.pdf> (accessed on 26 April 2016).

[11] Connorton (n 9), 291.

[12] European Parliament, Resolution on the interception of bank transfer data from the SWIFT system by the US secret services, P6_TA (2006)0317 (07 July 2006) note 2.

[13] ibid.

signed by the EU providing this derogation, and hence this programme lacked a legal basis under EU law.[14]

Following the media disclosure of the US TFTP, the role and responsibilities of SWIFT received much attention. Since SWIFT was headquartered in Belgium, it was bound both by EU and Belgian law on data protection.[15] An investigation initiated by the Belgian Data Protection Commissioner showed that SWIFT was a data controller and hence was responsible to ensure that the onward transfer of personal data to the US Treasury would be in compliance with the data protection legislation.[16] However, SWIFT was found to be acting contrary to the data protection provisions, such as the obligation to provide information to the data subject, the ban on transferring personal data to a third country unless that country provides an adequate protection for that data, and the independent control requirement.[17]

As a partial solution, SWIFT adopted principles in compliance with the then valid Safe Harbour Agreement, which regulated personal data transfer between the EU and US on data use.[18] Concurrently, being pressured by the EU, SWIFT representatives modified the technical structure of SWIFT and created a new operation centre in Switzerland, enabling the EU-originated financial data to be kept within the EU.[19] This modification prevented financial data transfer to the US Treasury within the US TFTP because this data would no longer be covered by the US law or by the subpoenas.[20] However, this prevention did not end the talks on financial data transfer because the EU and the US had already initiated negotiations for an agreement allowing this transfer in order to avoid losing access to financial data.[21]

B. The Legislative Procedure for the Terrorist Finance Tracking Program Agreement

Negotiations for an international financial data transfer agreement with the US ended on 30 November 2009 when the first Terrorist Finance Tracking Program Agreement (TFTP-I) was signed between the EU and the US.[22] The conclusion of the TFTP-I was based on the

---

[14] Cian C. Murphy, EU Counter-Terrorism Law Pre-Emption and the Rule of Law (Hart Publishing 2012) 153.

[15] ibid., 150.

[16] Belgian Data Protection Commission, Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas (nonofficial and temporary translation), <http://www.steptoe.com/assets/attachments/2644.pdf > (accessed on 26 April 2016).

[17] Belgian Data Protection Commission, 'Opinion No. 37/2006 of 27 September 2006' (n 15), 13. See also; Article 29 the Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the society for Worldwide Interbank Financial Telecommunication (SWIFT) (Opinion 10/2006), 01935/06/EN WP128 (Brussels, 22 November 2006), 26.

[18] Matthew R Van Wasshnova, 'Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned From the Existing System of Financial Information Exchange' (2008) 39 Case W Res J Int'L L 827, 846.

[19] Anthony Amicelle, 'The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From criticism to imitation of dataveilance' CEPS Paper in Liberty and Security in Europe, No 56 (CEPS August 2013) 5-6.

[20] Marise Cremona, 'Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of EU-US SWIFT Agreement', Austrian Academy of Science, Working Paper No. 04/2011, March 2011, 13.

[21] Kristin Archick, 'US-EU Cooperation against Terrorism', Congressional Research Service Report for Congress (2013) 13; Valentin Pfisterer, 'The Second SWIFT Agreement between the European Union and the United States of America- An Overview' (2010) 11 German Law Journal 1173, 1177; Murphy (n 14), 153-154.

[22] European Council Decision on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (Decision on the TFTP-I), 2010/16/CFSP/JHA, (30 November 2009).

former Articles 24 and 38 of the TEU[23], which required the Council to conclude an international agreement for law enforcement purposes and hence at the initial step the EU Parliament could not become involved with the conclusion of the TFTP-I.[24]

However, this chosen procedure was amended when the Treaty of Lisbon entered into force on 1 December 2009.[25] Being empowered on the approvals of international agreements[26] the EU Parliament rejected the conclusion of the TFTP-I on 11 February 2010 on the basis of its incompatibility with the right of EU citizens' personal data protection and privacy.[27] Following the rejection, the Council decided to conclude a second agreement, known as the TFTP-II.[28] This second agreement was criticised as being unsatisfactory for its non-compliance with EU data protection legislation.[29] Nevertheless, the EU Parliament approved the TFTP-II on 13 July 2010 and the Agreement came into force on 1 August 2010.[30]

C. The Operative Part of the Terrorist Finance Tracking Program Agreement

The TFTP-II operates as 'a system of mutual messaging between the EU Member States and the US.'[31] The system basically consists of transferring the financial data from the EU branch of SWIFT to the UST every month.[32] The UST shall identify in its request for obtaining data as clearly as possible that the data are necessary for combating terrorism or terrorist financing, clearly substantiate the necessity of the data, and the request shall 'be tailored as narrowly as possible in order to minimise the amount of data requested.'[33] The

[23] ibid. Article 24 required the Council the competence to authorise the Presidency of the EU to open negotiations for international agreements that later to be concluded by the Council. Article 38, therefore, provided the procedure to be followed for the conclusion of international agreements that fell under the scope of former third pillar. See; M. Quesada Gamez and E. Micheva, 'No Data without Protection?' 288-312, 291 in: Paul James Cardwell (ed), EU External Relations Law and Policy in the Post-Lisbon Era (Springer 2012).

[24] Murphy (n 14), 154. For more information on the data protection for law enforcement within the EU's former pillar structure see; Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?' (2009) 46 CMLR 1485.

[25] Treaty of Lisbon [2007] OJ C 306/1.

[26] Treaty on the Functioning of the European Union Article 218(6).

[27] European Parliament, 'SWIFT: European Parliament votes down agreement with the US', (11 February 2010) Press Release <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//EN> (accessed on 26 April 2016). See also; Archick (n 21), 10. For the purpose of our subject, this rejection was argued as being concrete evidence that the Parliament was determined to shape the content of the information exchange for countering terrorism Gamez and Micheva (n 23), 296. For more general information on the effect of the Parliament's rejection see, Jörg Monar, 'The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications' (2010) 15 European Foreign Affairs Rev 143.

[28] Murphy (n 14), 154.

[29] EDPS, Opinion on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (TFTP-II) (Opinion of the TFTP-II), (22 June 2010). For more information on the EDPS see; <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS>.

[30] Agreement between the European Union and the United States of America on the Processing and transfer of Financial Messaging Data From the European Union to the United States for the purposes of Terrorist Finance Tracking Program, OJ L 95/5 (27 July 2010).

[31] Pfisterer (n 21), 1184.

[32] Murphy (n 14), 155.

[33] The TFTP-II (n 30), Article 4(2).

task of verifying whether such requests are made in accordance with TFTP-II is given to Europol.[34]

The TFTP-II provides that access to data must be permissible only if there is clear evidence that the subject of the search has 'a nexus to terrorism or its financing.'[35] Although the concept of 'nexus to terrorism' is not defined in the Agreement, Article 2 contains a definition of terrorism on the same approach with the definition in the Council Framework Decision of 13 June 2002 on combating terrorism.[36] This in turn means that whereas the searches requested by the EU are subject to the EU definition of terrorism, the ones that are requested by the US are not.[37]

The TFTP-II introduces an oversight mechanism to ensure that the safeguards provided in the Agreement are respected.[38] In this regard, independent overseers may review in real time and retrospectively the searches put in place by the US Treasury, query the searches and request additional justification of the terrorism nexus.[39] Moreover, if any search is in breach of the safeguards guaranteed under Article 5 of the TFTP-II, the overseer has the authority to block it.[40]

D. The Proposal on the Establishment of a European Finance Tracking System

The TFTP-II has sparked debate from various stakeholders regarding its lack of conformity with the right to privacy and data protection. Having this in mind, the willingness for an equivalent European finance tracking system might seem to be an inconsistency of the EU policy. Yet the reasons in favour of such a system have revolved around the continuation of the EU's contribution to fight against terrorism and its financing within the EU, while ensuring the elimination of the large amount of personal data transfer to third countries.[41]

The Commission identified in its communication of November 2013 the options for creation of a possible European TFTP.[42] In this communication four out of ten options for the creation of such a system were disregarded on the grounds that they were not practical both from a technical and legal view.[43] Therefore, the Commission considered the impacts of a possible EU system on fundamental rights, and the cost effectiveness of establishing the system. Consequently, it took the view of not concluding a legislative proposal for the introduction of an equivalent European system.[44]

---

[34] ibid, Article 4(4).
[35] ibid, Article 5(5).
[36] EDPS, 'Opinion of the TFTP-II' (n 29), 3.
[37] Murphy (n 14), 156.
[38] Pfisterer (n 21), 1185.
[39] The TFTP-II (n 30), Article 12(1).
[40] ibid.
[41] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions a European terrorist finance tracking system: available options (Communication on a European terrorist finance tracking system: available options), COM (2011) 429 final (Brussels, 13 July 2011) 2.
[42] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions a European terrorist finance tracking system: available options (Communication on a European terrorist finance tracking system: available options 2013), COM (2013) 842 final (Brussels, 27 November 2013).
[43] Mara Wesseling and Marieke de Goede, 'Evaluation of EU measures to combat terrorism financing', LIBE Committee Studies, (11 April 2014) 29.
[44] European Commission Staff Working Document, Impact Assessment Accompanying the Document Communication from the European Commission to the European Parliament and the Council on a European Terrorist Financing Tracking System (TFTS), SWD(2013) 488 final, (Brussels, 27 November 2013) 36-37.

A possible European TFTP system limits the enjoyment of fundamental rights of individuals. Therefore, to what extent the creation of such a system is necessary must be examined in line with the needs of a democratic society and the rule of law. Otherwise, a European TFTP system cannot go further than being just another brick in the wall of surveillance.

3. EU-US Passenger Name Records Agreement

Passenger Name Records (PNR) is the name given for data sets that are created by airlines each time a passenger books a journey.[45] These data sets are kept in the airlines' reservation systems and contain a range of information such as name and date of birth of the passengers, date of reservation, travel agency through which tickets were bought, credit card number and even information about earlier bookings such as any required medical assistance and choice of meal.[46] The collection of PNR data has been done for commercial purposes, but the aftermath of the September 11, 2001 attacks gave momentum for its collection in order to 'identify dangerous passengers and take appropriate measures.'[47]

This part of the article explains the background of PNR data transfers from the EU to the US law enforcement authorities for countering terrorism and the agreements concluded for that purpose. Whilst making an analysis of the scope of the Agreement in effect for the time being, it aims to provide a general backdrop for the question of its compliance with the right to privacy and data protection at least from the EU perspective.

A. The Background to the Agreements

As a response to the September 2001 attacks, the US authorities started to employ counter-terrorism measures to control borders and in November 2001 the US administration passed the Aviation and Transportation Security Act (ATSA).[48] The ATSA introduces an obligation for each international air carrier operating a passenger flight in foreign air transportation to the US to provide the US Bureau of Customs and Border Protection (CBP), which is now a department of the US Department of Homeland Security (DHS), electronic access to the specific data relating to passengers and crew.[49] Another obligation for airlines is to provide passenger name records available to CBP upon request.[50] Non-compliance with this obligation can lead to airlines paying fines or losing their landing rights.[51]

The requirements provided under ATSA created a conflict with the EU principles protecting the right to privacy and data protection. The obligation for European airline companies to provide PNR data to the CBP was in contradiction with Article 25 of the Data Protection Directive 95/46 in which the transfer of data to a third country is only allowed if

[45] For more information see, European Commission, 'The Passenger Name Record (PNR): Frequently Asked Questions', (13 July 2007) Press Release <http://europa.eu/rapid/press-release_MEMO-07-294_en.htm?locale=en> (accessed on 26 April 2016).
[46] Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of Passenger Manifest Information and other data from the Airlines to the United States (Opinion 6/2002), 11647/02/EN WP 66 (24 October 2002) 3.
[47] Michele Nino, 'The protection of personal data in the fight against terrorism New perspectives of PNR European Union instruments in the light of the Treaty of Lisbon' (2010) 6 Utrecht Law Review 62, 63. For remarks on the comparison between the PNR and Advanced Passenger Information see, HL Select Committee on European Union 21st Report (HL Paper 2006-7) 9.
[48] Aviation and Security Act (ATSA), 19 November 2001 (Public Law 107-71, 107th Congress).
[49] ATSA sec. 115(c)(1).
[50] ibid, 115(c)(3).
[51] Van Wasshnova (n 18), 833.

that country ensures an adequate level of protection.[52] At that point it was not clear whether the US authorities could provide this protection since an adequacy assessment had not been made before the conclusion of EU-US PNR agreements.[53] As was observed by the Article 29 Data Protection Working Party (Working Party) the EU's data protection authority, the implementation of the then valid Safe Harbour Agreement was also not an appropriate option, for this agreement could not apply 'for the protection of data transfers to government authorities.'[54] Consequently, European airline companies were forced to choose to abide either by the EU law on data protection or by ATSA. On one hand, if these companies had chosen to abide by the latter, they would have acted contradictory to the EU data protection legislation and have had to face sanctions imposed by European data protection authorities.[55] On the other hand, if they had chosen to abide by the former, they would have faced sanctions as required under ATSA.

In its communication of December 2003, the Commission offered a two-step approach to solve the problem.[56] The first step was the adoption of an adequacy decision by the Commission on the US processing of PNR data and the second step was to accompany this decision with a bilateral international agreement.[57] The Commission put forward this legal solution assuming that even though the subsequent use of PNR data by US authorities was for law enforcement purposes, the initial collection of this data by European airlines was for commercial purposes and thus would fall within the context of commercial processing, rather than processing for law enforcement.[58] Departing from this assumption, the Commission took the view that PNR data transfer would be a matter falling under the scope of the former first pillar rules[59] in which the Commission would have the competence to enter into negotiations with the US.[60] After all these steps were fulfilled, a bilateral agreement on PNR transfers, the 2004 PNR Agreement, between the US and the Commission on behalf of the Community was signed on 28 May 2004, which entered into force on the same day.[61]

Although the Council and the Commission carried out the negotiations for both of these instruments with the assumption that they had the competence to do so in the context of Community law for data protection[62], the then-named European Court of Justice's (ECJ) annulment decision on the 2004 PNR Agreement gave a different dimension to the issue.

B. The Annulment Decision by the European Court of Justice

[52] Article 29 of the Data Protection Working Party, Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, DG XV D/5025/98 WP 12 (24 July 1998) 3.
[53] Murphy (n 14), 159.
[54] Article 29 Data Protection Working Party, 'Opinion 6/2002' (n 46), 6.
[55] Nino (n 47), 71.
[56] European Commission, Communication to the Council and the Parliament on Transfer of Air Passenger Name Records (PNR) Data: A Global EU Approach (Communication on a global approach), COM (2003) 826 final (Brussels, 16 December 2003).
[57] ibid, 2.
[58] Vagelis Papakonstantinou and Paul de Hert, 'The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on Either Side of the Atlantic', (2009) 46 CML Rev 885, 901.
[59] Paul Craig and Gráinne de Búrca, EU Law: Text, Cases, and Materials (Oxford University Press 2011) 13.
[60] Papakonstantinou and de Hert (n 58), 901.
[61] Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 142M, (30 May 2004).
[62] Paul de Hert and Serge Gutwirth, 'Data Protection in the Case law of Strasbourg and Luxemburg: Constitutionalisation in Action' 3-44, 34 in Serge Gutwirth et al (eds), Reinventing Data Protection (Springer 2009).

Only a few months after the conclusion of the 2004 PNR Agreement, on 27 July 2004, the EU Parliament sought annulment of two decisions upon which this agreement was based: the Commission's Adequacy Decision and the Council decision on the authorisation for signing the Agreement.[63] On 30 May 2006, the ECJ made its decision; it annulled both decisions on the grounds that the processing of PNR data under the 2004 PNR Agreement was for law enforcement purposes, not for commercial purposes as the Commission and Council claimed and neither of these two EU bodies were competent to adopt decisions on a law enforcement basis.[64]

The Council responded to the ECJ's annulment decision with the Interim Agreement, later to be replaced by the 2007 PNR Agreement.[65] Both these agreements were based on Articles 24 and 38 of the TEU in the context of the former third pillar procedure, the same basis as the TFTP-II.[66] As mentioned earlier in the TFTP-II, this legal basis prevented the EU Parliament from having the legislative role in the adoption of international agreements on law enforcement.[67] Likewise, the ECJ also did not have judicial control.[68] Hence, this legal basis had an effect on the democratic and judicial control of these two agreements.[69]

C. The 2012 PNR Agreement

The 2007 PNR Agreement explicitly stated its own expiration date as 'seven years after the date of signature unless the parties mutually agree to replace it.'[70] This provision allowed the competent authorities to negotiate on a new agreement.[71] Despite the criticisms on the flaws of this new agreement, known as the 2012 PNR Agreement, on the exercise of the right to privacy and data protection[72], the EU Parliament adopted it and the Agreement entered into force on 1 July 2012.[73]

---

[63] Papakonstantinou and de Hert (n 58), 902.

[64] Joined cases Case C-317/07 and C-318/04, *European Parliament v. Council of the European Union* (C-317/04) and European Parliament v. Commission of the European Communities (C-318/04), [2006] ECR I-4721 (hereinafter, The Joined Cases CJEU) paras. 56-70. In the pertinent part of the 15th preamble to the decision on adequacy explicitly states that "… PNR data will be used strictly for purposes of preventing and combating: terrorism and related crimes; other serious crimes, including organised crime, that are transnational in nature; and flight from warrants or custody for those crimes". See also Murphy (n 14), 160-161.

[65] Agreement between the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) OJ L 204 (04 July 2007).

[66] Murphy (n 14), 161.

[67] ibid, 162.

[68] ibid.

[69] ibid.

[70] The 2007 PNR Agreement (n 65), note 9

[71] European Commission, Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, COM(2011) 807 final (Brussels, 28 November 2011).

[72] Article 29 Working Party, Open Letter to the Members of the LIBE Committee of the European Parliament (Brussels, 6 January 2012); EDPS, Opinion on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (Opinion on the 2012 PNR Agreement), (Brussels, 09 December 2011); EDRi.org, 'Is the new EU-US PNR Agreement acceptable?' (01.2012) <http://edri.org/files/2012EDRi_US_PNRcomments.pdf> (accessed on 21 February 2016).

[73] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, OJ L 215/5 (11 August 2012).

D. The Scope of the 2012 PNR Agreement

In general, the 2012 PNR Agreement, like its predecessors, lays down the rules for the processing of PNR data by the US authorities. To be more precise, the purpose of this processing is explicitly stated as being 'for the purposes of preventing, detecting, investigating and prosecuting (a) terrorist offences and related crimes and (b) crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.'[74] Moreover, the Agreement introduces the processing of PNR data 'on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.'[75]

The 2012 PNR Agreement contains nineteen types of data to be transferred to the US, like the 2007 PNR Agreement.[76] As for the processing of 'sensitive data'[77] it is important to recall the 2007 PNR Agreement in which the DHS was permitted to use sensitive data 'in an exceptional case where the life of a data subject or of others could be imperilled or seriously impaired.'[78] The 2012 PNR Agreement further provides that in cases in which the PNR data includes sensitive data, the DHS shall employ automated systems to filter and mask out this data from PNR.[79] This being said, as under the 2007 PNR Agreement, the sensitive data might be used for exceptional cases.[80] Additionally, the new agreement introduces the storage of such data for at least 30 days.[81]

Another crucial point is the retention period of the PNR data provided under the new agreement. The 2007 Agreement was criticised as allowing the PNR data to be held in the US system for almost 5 years and therefore the EU Parliament asked for a limitation of this retention period.[82] Unfortunately, the 2012 PNR Agreement provides a retention period of almost 15 years, a much more extensive period of time than the former agreement required.[83]

As far as the method of PNR data transfer is concerned, the 2012 PNR Agreement reflects the previous agreement by requiring the use of a push method.[84] This method is distinct from a pull method. Whereas air carriers send the PNR data to the DHS with the push method, the pull method permits the DHS to require access to the PNR data from air carriers' systems.[85] The push method, according to the Commission's Communication of December 2003, is a computer-based filter system that allows 'the data flows from the airlines or reservation systems to the US security authorities to be controlled in the EU and … limit the transfer to what is strictly necessary for security purposes.'[86] Especially the last part of this statement is the very reason why such a method was considered by the Working Party as being 'the only way of transferring personal data.'[87] Like the previous agreement,

---

[74] ibid, Article 4(1).
[75] ibid, Article 4(2).
[76] The 2012 PNR Agreement (n 73), Annex.
[77] For more information about the concept of sensitive data see, Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136 (20 June 2007), 6-7.
[78] Letter from Michael Chertoff, Secretary of Homeland Security to Luis Amado, President of the Council of the European Union (undated), OJ L 2004/18 (4 August 2007), Title III.
[79] The 2012 PNR Agreement (n 73), Article 6(1).
[80] ibid, Article 6(3).
[81] ibid, Article 6(4).
[82] European Parliament, Resolution on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada (Resolution of 5 May 2010), P7_TA (2010)0144 (05 May 2010), note 9(a).
[83] Article 29 Data Protection Working Party, 'Open Letter to the LIBE Committee' (n 72).
[84] The 2012 PNR Agreement (n 73), Article 15.
[85] Papakonstantinou and de Hert (n 58), 912.
[86] European Commission, 'Communication on a global approach' (n 56), note 3.3, 8.
[87] Article 29 Data Protection Working Party, Opinion 5/2007 on the follow-up agreement between the European

the 2012 PNR Agreement also gives the air carriers two years to implement this technical ability.[88] Although the requirement for a push method is welcome, the new agreement still requires carriers to provide access to PNR data in exceptional cases or where they are technically unable to respond to the requests made by the DHS.[89] This in turn was criticised by the Working Party as not being clear on under what conditions such access should be allowed.[90]

E. The Proposal on the Establishment of a European Passenger Name Record Agreement

The idea of establishing an EU PNR system dates back to 2004[91] and since then the need for such a system has been the subject of contentious discussions. The push for the establishment of such a system accelerated after the terrorist attack that targeted the French satirical weekly magazine Charlie Hebdo's headquarters in Paris in January 2015.[92] The primary calls for establishing an EU PNR system were made by the European Counter-Terrorism Coordinator, the Commissioner for Migration, Home Affairs and Citizenship on behalf of the Commission and under the Riga Joint Statement of EU Ministers for Justice and Home Affairs.[93] Consequently, after much contention in the EU Parliament, the draft rules on an EU PNR system were approved by the EU Parliament's Civil Liberties Committee and this approval enabled the initiation of negotiations between the EU Parliament, Council and Commission for a draft EU PNR system agreement.[94]

The concerns over the establishment of an EU PNR system resemble those over an EU Terrorist Finance System. Therefore, the crux of the matter is to ensure that the necessity and proportionality of such a system is well-established, for these measures have negative repercussions for the fundamental rights of individuals. Additionally, as the thriving effects of the Snowden revelations in June 2013 surrounding the US measures and the subsequent allegations on the infringement of the rights of EU citizens' still lingers, the adoption of an EU-PNR system must be reconsidered.

4. Evaluation of the Agreements with Right to Privacy and Personal Data Protection

The TFTP-II and 2012 PNR Agreement highlight their commitments to the right to privacy and personal data protection by explicitly referring to the related articles of treaties and international agreements. Whether the TFTP-II and the 2012 PNR Agreement are consistent

---

Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security (Opinion 5/2007), 01646/07/EN WP 138 (17 August 2007) 11.

[88] The 2012 PNR Agreement (n 73), Article 15(4).

[89] ibid, Article 15(5).

[90] Article 29 Data Protection Working Party, 'Open Letter to the Members of the LIBE Committee' (n 72).

[91] European Council, 'Declaration on Combating Terrorism', (25 March 2004) <http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf> 8, (accessed on 26 April 2016).

[92] See generally 'Charlie Hebdo attack: Latest news and comment on Charlie Hebdo attack in Paris', The Guardian, <http://www.theguardian.com/world/charlie-hebdo-attack> (accessed on 26 April 2016).

[93] For a general overview of EU policy response to terrorist attacks in Paris, see; Didier Bigo et al., 'The EU Counter Terrorism Policy Responses to the Attack in Paris: Towards an EU Security and Liberty Agenda', CEPS Paper in Liberty and Security in Europe, No 81 (CEPS February 2015).

[94] European Parliament, Passenger Name Records: MEPs back EU system with data protection safeguards (15 July 2015), Press Release, <http://www.europarl.europa.eu/news/en/news-room/content/20150714IPR81601/html/Passenger-Name-Records-MEPs-back-EU-system-with-data-protection-safeguards> (accessed on 26 April 2016).

with EU citizens' fundamental rights and the interference caused by these agreements can be justified for the pursuit of countering terrorism, are other issues to be discussed. This part aims to find answers to those questions.

This part will focus on the CJEU's *Digital Rights Ireland* decision, because this decision illustrates the compliance of the data retention measures with the Charter and can give some guidance as to the CJEU's approach on what amounts to an interference in the context of these retention measures in particular, and surveillance measures in general.[95]

A. The Right to Privacy in the EU

Article 8(1) of the European Convention on Human Rights (ECHR) states that 'Everyone has the right to respect for his private and family life, his home and his correspondence.' Article 7 of the Charter of Fundamental Human Rights of the European Union (Charter) resembles Article 8 of the ECHR except that the expression 'correspondence' is replaced with 'communications.'[96] This resemblance is important because according to Article 52(3) of the Charter, for rights which correspond to the rights guaranteed under the ECHR, the meaning and the scope of those rights shall be the same as those laid down by the ECHR.[97] Since privacy is one of those corresponding rights, Article 7 of the Charter must therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case-law of the European Court of Human Rights (ECtHR).[98]

The ECtHR's interpretation of Article 8(1) of the ECHR has been crucial in the development of the right to privacy in the EU before the Charter existed. Before the Charter became binding the CJEU developed the protection of privacy in particular and fundamental rights in general by referring to the ECHR as the general principles of Community Law, having the same validity as primary law.[99] Moreover, all EU Member States are signatory parties to the ECHR and hence they have to secure to everyone within their jurisdiction the rights and freedoms provided in the Convention.[100]

In light of the above, the CJEU has been embracing the same aspects of privacy as interpreted by the ECtHR.[101] Of great importance for our subject the CJEU mentions the

---

[95] Digital Rights Ireland CJEU (n 2). In this decision the CJEU dealt with the lawfulness of the Data Retention Directive 2006/24. According to this Directive, the telecommunication companies were obliged to retain the communication related data of all subscribers and users for up to two years or more to be used for law enforcement purposes. See Data Retention Directive 2006/24/EC Article 1 and Article 6. However, the CJEU found this data retention measure to be in contravention to Articles 7 and 8 of the Charter and therefore it declared the directive invalid. For a comprehensive work on the judgment, its impact in the existing data processing measure employed for law enforcement purposes and the recommendations for EU policy-makers see; Franziska Boehm and Mark D Cole, 'Data Retention after the Judgment of the Court of Justice of the European Union', <http://www.greens-efa.eu/data-retention-12640.html> (accessed on 26 April 2016); Elspeth Guild and Sergio Carrera, 'Digital Rights Ireland and the Trail of the Data Retention Directive', CEPS Paper in Liberty and Security in Europe, No 65 (CEPS May 2014).

[96] This replacement of 'correspondence' to 'communication' was not done intentionally and hence does not carry a different meaning. Boehm and Cole (n 95), 21, footnote 52.

[97] Charter, Article 52(3).

[98] C-400/10 J. Mc.B v. L.E. EU:C:2010:582 [2010] para 53.

[99] Hans Christian Krüger, 'The European Union Charter of fundamental Rights and the European Convention on Human Rights: An Overview', xvii-xxvii, xxi in Steve Peers and Angela Ward (eds), The European Union Charter of Fundamental Rights (Hart Publishing, 2004).

[100] ECHR, Article 1.

[101] For more comprehensive information on the jurisprudence of both the CJEU and the ECtHR on privacy and data protection see; Juliane Kokott and Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR' 3 International Data Privacy Law 222.

ECHR and case-law of the ECtHR and departs from the ECtHR's broad interpretation of 'private life'[102] to cover cases concerning data protection.[103]

B. The Right to Personal Data Protection in the EU

Personal data protection has been acknowledged by the ECtHR as an aspect of privacy protection and is enshrined in Article 8 of the ECHR.[104] Article 7 of the Charter resembles this article of the ECHR, but Article 8 of the Charter also puts something more to data protection and recognises it as a separate fundamental right, next to privacy.[105] Furthermore, this Article lays down safeguards specifically for data protection and states that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some legitimate basis laid down by the law.[106] A right to access to data that has been collected concerning them was given to individuals, and they also have the right to rectify this data.[107] An independent authority shall control compliance with these rules.[108]

The CJEU also recognises data protection as a fundamental right, but despite the Charter's approach on giving this right an autonomous nature, in most cases the CJEU is

[102] 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.' Niemitz v. Germany, (1992) 16 EHRR 97, para 29.

[103] See Joined Cases C-465/00, C-138/01, Österreichischer Rundfunk, EU:C:2003:294 [2003] ECR I-4989, paras. 72-75; Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen EU:C:2010:662 [2010] ECR I-1 1063 para. 47

[104] In Leander v. Sweden, the Court held that storing and the release of information relating to an individual's private life amounted an interference with right to privacy as guaranteed under Article 8 of the ECHR, at para 48.. Even if the information does not relate to an individual's private life and can be considered, in the Court's words, as 'public information', the ECtHR has held in many of its decisions that this information also fell within the scope of private life 'where it is systematically collected and stored in files held by authorities', especially in cases where such information 'concerns a person's distant past.' Rotaru v. Romania, App no. 28341/95 (ECtHR 4 March 2000) para 43; MM v. UK App no 24029/07 (ECtHR 13 November 2012) para 187; Cemalettin Canlı v. Turkey App no. 22427/04 (ECtHR 18 November 2008) para 33. The ECtHR also referred to existing data protection treaties to explain what 'personal data' is. Amann v. Switzerland, App no. 27798/95 (ECtHR 16 February 2000) para 65; Rotaru v. Romania (n 109) para 43; MM v. UK (n 109) para 188.

[105] Charter, Article 8(1). Suffice it to say here that there has been an ongoing debate on the relationship between the data protection and privacy. Many legal scholars, acknowledging the interaction and overlap between these two rights, are concerned with assessing data protection, and values underlined specifically by it, on their own, with a little less reference to privacy. See Generally Paul de Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in Erik Claes, Anthony Duff and Serge Gutwirth (eds), Privacy and the Criminal Law (Intersentia 2006); Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so new right' 3 International Data Privacy Law 88; Christopher Kuner, 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) Computer Law & Security Review 307.

[106] Charter, Article 8(2).

[107] Ibid.

[108] Ibid.

reluctant to consider data protection without referring to the right to privacy.[109] In its *Schecke* decision, the CJEU referred to the relevant data protection provision in the Charter, but further clarified data protection as being 'closely connected with the right to respect of private life expressed in Article 7 of the Charter.'[110] It further combined data protection with privacy by stating that any information relating to an identified or identifiable individual[111] is a concern of 'the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter.'[112]

In brief, despite the CJEU's approach on combining data protection with the right to privacy, the Charter gives constitutional recognition to data protection as a separate fundamental right.[113] This recognition reinforces personal data protection's position against the activities such as collection, storage and transfer of data, because such activities can be lawfully permissible if they satisfy the protection requirements arising from Article 8 of the Charter.[114]

C. Relevance of the Right to Privacy and Personal Data Protection with the TFTP-II and the 2012 PNR Agreement

When examining the legality of the TFTP-II and the 2012 PNR Agreement in relation to fundamental rights, one must first detect under which of these rights' protective ambit the two agreements fall. The CJEU approach on measures pertaining to data processing and their relevance to fundamental rights is well-demonstrated in the Court's *Digital Rights Ireland* case. In this case, the CJEU observed that data retained from the providers of publicly available electronic communications services of public communication networks:

> taken as a whole, may allow very precise conclusions to be drawn concerning private lives of the persons whose data has been retained, such as the habit of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[115]

Therefore, the CJEU found the retention of the data in question 'for the purpose of possible access to them by the competent authorities, as provided for by Directive 2006/24' to

[109] Tzanou (n 105), 94. Suffice it to say here that data protection has been linked with the protection of individuals' rights and freedoms such as freedom from discrimination and freedom of expression, but mostly a special importance to privacy has been given on the basis that unlawful processing may lead to interference with an individual's private life. After making this observation Bygrave argues that privacy has been the prominent fundamental right to be linked with data protection due to the fact that data protection legislation emphasised the protection of that right central to their aim. See; Lee A Bygrave 'Privacy Protection in a Global Context' (2004) 47 Scandinavian Studies in Law 319, 332. The Data Protection Directive recognises the importance of privacy in the discourse of data processing. According to this directive, particular importance shall be given to individuals' right to privacy with respect to the processing of personal data by the EU Member States. See; Data Protection Directive 95/46, Article (1).

[110] Schecke CJEU (n 103), para 47.

[111] Data Protection Directive 95/46, Article 2(a).

[112] Schecke CJEU (n 103), para 52.

[113] Tzanou argues that the reason why data protection is not assessed independently from the right to privacy is embedded in the way this protection is formulated in the Charter as a tool aimed at regulating the power, but not prohibiting it. The author also suggest how to reconstruct the data protection so that it can operate on its own. For the author's argument on the issue see; Tzanou (n 105), 97.

[114] Schecke CJEU (n 103), para 47.

[115] Digital Rights Ireland CJEU (n 2), para 25-27.

'directly and specifically' affect 'private life and consequently, the rights guaranteed by Article 7 of the Charter.'[116]

As for data protection, the CJEU stated that retention of data constituted data processing and hence fell under Article 8 of the Charter.[117] It further reiterated its settled case-law that any data processing falling within the scope of Article 8 of the Charter must satisfy the protection requirements arising from it.[118]

Along the same line, the TFTP-II directly affects privacy in that the financial data required by this agreement can reveal the private lives of individuals.[119] It is also evident that financial data constitutes personal data as it relates to 'any information relating to an identified or identifiable person.'[120] Thus, the retention of financial data constitutes processing of personal data. Therefore, the data processing activities required by the TFTP-II fall within the scope of right to privacy and personal data protection as guaranteed under the Charter. The same conclusion can be drawn for the PNR data transfer.[121]

D. Interference with the Right to Privacy and Personal Data Protection

According to the CJEU, a finding of an interference with the right to privacy does not necessitate that the information on the private lives of individuals is sensitive or that the individuals have been inconvenienced by its retention.[122] Therefore, merely the retention of data constitutes an interference with the right to privacy.[123] The CJEU also considers access by competent authorities to the data as a further interference with the same right.[124] In brief, the CJEU establishes the existence of an interference with the right to privacy in two scenarios; first the data must be retained; and second the data must be accessed by the competent authorities.

The 2012 PNR Agreement obliges European airline companies to retain data about individuals and hence it constitutes an interference with the right to privacy as guaranteed under Article 7. Along the same lines, the TFTP-II provides the retention of financial data for their subsequent transfer from SWIFT to the UST and therefore interferes with the same right. Moreover, TFTP-II lays down the rules for enabling competent US law enforcement authorities to get access to the financial data. The 2012 PNR Agreement also grants such access for the PNR data. Therefore, an interference with the right to privacy occurs under both agreements.

As for establishing an interference with personal data protection, the CJEU is of the opinion that if an activity provides for the processing of data, such activity interferes with the right to personal data protection guaranteed under Article 8 of the Charter.[125] The TFTP-II and the 2012 PNR Agreement provide rules for data processing and therefore interfere with the said Article.

The discourse on the interferences of the TFTP-II and 2012 PNR Agreement is also anchored to the Big Data issue in the digital age. 'Big Data' is the advanced ability to collect, harvest and analyse ample quantities of data by algorithms or automated processing. It

[116] ibid, para 29.
[117] ibid.
[118] ibid.
[119] It is important to note here that the CJEU considered the professional activities of individuals in the protective ambit of privacy, in line with the broad interpretation of private life made by the ECtHR. See; Schecke CJEU (n 103), para 59. See generally Kokott and Sobotta (n 101).
[120] Data Protection Directive 95/46, Article 2(a).
[121] See also Article 29 Data Protection Working Party, 'Opinion of 6/2002' (n 46), 4.
[122] Digital Rights Ireland CJEU (n 2), para 33; Österreichisher Rundfunk CJEU (n 103) para 75.
[123] Digital Rights Ireland CJEU (n 2), para 34.
[124] ibid, para 35.
[125] ibid, para 36.

undeniably has potential risks for privacy and data protection.[126] It runs counter to individuals' control over information, data protection principles such as data minimisation, and purpose limitation.[127] What is more, data mining[128] and profiling[129], especially if these practices are employed for the purpose of national security and countering terrorism, run the risk of stigmatisation of individuals. If public opinion is manipulated by the consequence of Big Data practices, these practices may also affect the freedom of expression of individuals.[130]

The negative repercussions of Big Data practices on fundamental rights culminate when those practices are used to permit surveillance.[131] Surveillance is, as Lyon describes, 'focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.'[132] Concerning freedom of expression in the discourse of surveillance measures, an individual will not express his or herself if he or she is subjected to surveillance and hence will not enjoy this freedom.

The relevance of surveillance and freedom of expression came to the CJEU's attention in the *Digital Rights Ireland* case. Interestingly, Advocate General Cruz Villalón made some remarks in his opinion as to the fact that data retention measures may play a decisive role on the way European citizens exercise their freedom of expression as enshrined in Article 11 of the Charter and create a 'vague feeling of surveillance.'[133] This being settled, Villalón further stated that although a possible interference of data retention

---

[126] Omer Tene and Jules Polonetsky, 'Judged by the Tin Man: Individual Rights in the Age of Big Data', (2013) 11 J on Telecomm & High Tech L 351; David Lyon, 'Surveillance Snowden, and Big Data Capacities, consequences, critiques', Big Data & Society (July 2014) <http://bds.sagepub.com/content/1/2/2053951714541861> (accessed on 26 April 2016); Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74. Big Data practices have been applied for the purposes of health, consumer marketing, national security, and countering terrorism to name a few. Hence, the permissibility of these practices against the fundamental rights of the individual will differ depending on the purpose they are used for. See Omer Tene and Jules Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' (2012) 64 Stan L Rev Online 63, 67; Lyon, 'Surveillance Snowden, and Big Data Capacities, consequences, critiques' 2.

[127] Tene and Polonetsky ask whether data minimisation and purpose limitation are practical approaches to fulfil privacy concerns in the age of Big Data. See; Tene and Polonetsky, 'Judged by the Tin Man: Individual Rights in the Age of Big Data' (n 126), 362.

[128] As Rubinstein argues, data mining enables those who process data to discover previously unknown information from database and due to the secret nature of the decision made by data mining to data subjects, issues such as reliability and accuracy of data emerge. Rubinstein (n 126), 78.

[129] The CJEU was of the opinion that retention of wide-ranging data concerning the habits of everyday life, residence, daily movements, social relationship and social environment of people 'may allow very precise conclusions to be drawn concerning the private lives of the persons', or in other words pave the way for 'profiling' of individuals. See; Digital Rights Ireland (n 2), para 57.

[130] Tene and Polonetsky discuss the link between Big Data practices and freedom of expression, particularly political expression, by giving example of political campaigns in the US Presidential elections, where voters were targeted on the basis of merged information on their online identities and behaviours. Tene and Polonetsky, 'Judged by the Tin Man: Individual Rights in the Age of Big Data' (n 126), 360.

[131] Big Data practices are only one aspect of using information in the digital age to undertake surveillance. See Lyon, 'Surveillance Snowden, and Big Data Capacities, consequences, critiques' (n 126), 4.

[132] David Lyon, Surveillance Studies: An Overview (Cambridge Polity Press 2007) 14. Cameron takes the issue from the interest of 'national security' and illustrates the purposes of surveillance in general as obtaining intelligence on a suspect for use in further investigation and to obtain specific evidence of a crime and preventing of future crimes. Iain Cameron, National Security and the European Convention on Human Rights, (Martinus Nijhoff Publishers 2000) 86-90.

[133] Joined Cases C293/12 and C594/12 Digital Rights Ireland v. The Minister for Communications, Marine and Natural Resources and Others [2013] CJEU Opinion of AG Villalón para 52.

measures with freedom of expression may exist, the CJEU did not have sufficient material to give a ruling on such an interference and therefore it could only take the issue as a 'collateral consequence of interference with privacy.'[134] Just as Villalón reckoned, the CJEU used the notion of constant surveillance posed by data retention measures in order to demonstrate the seriousness of interferences with the right to privacy and data protection, but it did not consider the impact of that surveillance on individuals' freedom of expression. According to the Court, as Directive 2006/24 was annulled due to its breach of the right to privacy and data protection, it was unnecessary to examine further that Directive's validity in view of freedom of expression.[135]

In light of the above, it is possible to say that if the TFTP-II and the 2012 PNR Agreement are taken before the CJEU, the Court may not give a ruling on the interference of these agreements with freedom of expression. The same conclusion can be drawn from the cumulative effects of these agreements with freedom of association and freedom of movement. However, it is also important not to lose sight of the fact that a revision of surveillance measures with regard to freedom of expression is crucial to demonstrate the impact of these measures on fundamental rights.[136] Finally, issues such as data mining, profiling and minimisation of the risk of stigmatisation ought to be examined in the discourse of compliance with privacy and data protection, as examined below.

E. Compliance with Right to Privacy and Right to Protection of Personal Data

After establishing an interference, one must examine whether this interference can be justified according to Article 52 of the Charter. In this regard, any derogations and limitations on the exercise of rights must be 'provided by law, respect its essence, subject to the principle of proportionality and limitations to that right only if they are genuinely necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'[137] Then, the question is, do the TFTP-II and the 2012 PNR Agreement satisfy this set of rules and subsequently can the interference with EU citizens' right to privacy and personal data protection caused by those agreements be justified? To answer these questions, first one must ask whether the limitation is provided by law; and then one has to ask whether the limitation on the exercise of the right to privacy and data protection respects the essence of these rights. If this limitation is found to be in accordance with such respect, then one has to ask whether the limitation has an objective general interest. The final question which needs to be addressed is whether the general interest found to exist is proportionate, taking the extent of the limitations on the rights at stake into account. The interference can only be justified if these three questions are answered in the affirmative.

i) Provided by Law

The data processing activities in question are provided for by the TFTP-II and the 2012 PNR Agreement, two legislative acts of the EU, and hence the interference of these agreements with fundamental rights must be regarded as provided by law.[138]

---

[134] ibid.
[135] Digital Rights Ireland CJEU (n 2), paras 69-70.
[136] See Boehm and Cole (n 95), 27.
[137] Charter, Article 52(1).
[138] For AG Villalón's discussion in the case of *Digital Rights Ireland* about the notion of 'provided by law' being considered beyond a formal requirement and hence examining the 'quality of law' in alignment with the ECtHR see; Digital Rights Ireland Opinion of AG Villalón AG opinion (n 132) para 75. See also Boehm and Cole (n 94) 32-33.

ii) The Respect of the Essence of the Rights

Any limitations severely hampering the enjoyment of a right or preventing the fulfilment of the underlying core value of it, mean that such limitations do not respect the essence of the right. In other words, the exercise of a right is respected if a limitation on this right avoids completely eroding it. According to the CJEU, if an interference, regardless of how particularly serious it can be, does not adversely affect the essence of the rights limited, it does not infringe their essence and therefore 'the respect the essence of the rights' criteria is met.[139] Having said this, what seems to be not adversely affecting the essence of the right - such as the content of the retained data or principles on securing the data - was considered in the *Digital Rights Ireland* case by the CJEU in the context of the compatibility with the proportionality principle. Therefore, even if one assumes that the TFTP-II and the 2012 PNR Agreement do not infringe the essence of the right to privacy and data protection, they may, after meeting the objective of general interest test, be incompatible with the proportionality test.

iii) 'Countering Terrorism' as an Objective of General Interest

As mentioned, the main purpose of the TFTP-II and 2012 PNR Agreements is countering terrorism.[140] The essential question here is whether this purpose is sufficiently robust for both agreements to put at stake the right to privacy and personal data protection. The answer can be found with a reference to case-law of the CJEU. As the CJEU reaffirmed in *Digital Rights Ireland*, 'the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest.'[141] Keeping this in mind, even if the fight against terrorism would be considered as an objective of general interest for the TFTP-II and 2012 PNR Agreement, the next test for these privacy-intrusive agreements to be justified is to determine whether they comply with the proportionality principle.

iv) The Principle of Proportionality

The proportionality principle requires that any fundamental rights-intrusive measure does not 'exceed the limits of what is appropriate and necessary in order to achieve those objectives.'[142] According to the CJEU, when assessing whether the EU legislature acted in compliance with these principles, the extent of the EU legislature's discretion must be limited and must depend on 'the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference.'[143] Acknowledging the importance of the right to privacy and personal data protection for individuals, the CJEU observed that any limitations on the right to privacy and personal data protection must apply in so far 'as strictly necessary.'[144]

Leaning on the findings of the CJEU, the TFTP-II and 2012 PNR Agreements will now be assessed separately in order to determine whether they are proportionate and

[139] Digital Rights Ireland (n 2) paras 39-40.
[140] See Chapters 2 (C) and 3 (D) of this article.
[141] Digital Rights Ireland CJEU (n 2), para 42. Departing from the concept of 'national security', the Working Party discuss that this concept used by national authorities cannot automatically be presumed to exist and hence the national security exception must be well-demonstrated when measures adopted for such exception limit fundamental rights. See; Article 29 Data Protection Working Party, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215 (10.04.2014) 6.
[142] Digital Rights Ireland CJEU (n 2), para 46 (Emphasis added).
[143] ibid, para 47.
[144] ibid, para 52 (Emphasis added).

necessary for countering terrorism and whether those two privacy-intrusive agreements can be justified.

The Terrorist Finance Tracking Program Agreement

While a restrictive measure meets an objective of general interest, one should not assume that this measure would be legitimate. The second step for the legality test of such a measure is to verify its proportionality.[145] In this regard a restrictive measure can only be justified if it is appropriate to attain the legitimate objectives pursued, and does not exceed the limits of what is appropriate and necessary in order to achieve these objectives.[146] The CJEU considers data retention measures as 'appropriate' tools to counter terrorism.[147] If a measure is found to be 'appropriate', then this measure must be necessary for a pursued objective interest to meet the proportionality test. One way to assess the necessity of a privacy-intrusive measure is to review if the same pursued objective interest can be achieved by other instruments that are less intrusive of the right to privacy and personal data protection. This matter came to the EDPS's attention, which pointed out that there were other existing EU and international agreements on the exchange of information for third countries. It emphasised that the TFTP-II was another agreement to require such exchange, and therefore it was important to show sufficient evidence 'to which extent the agreement is really necessary in order to obtain results that could not be obtained by using less privacy-intrusive instruments.'[148]

The necessity of the TFTP-II would only be sufficiently established if there was sufficient information on its implementation. It is unfortunate that while recalling the usefulness of the US TFTP, the UST has repeatedly raised concerns over the harm that might be caused if more detailed information of the program was to become public and therefore it has not provided sufficient information on transferred data volumes.[149] This is a major obstacle to the clarification of the necessity of the TFTP-II. This being said, so as to evaluate EU measures to combat terrorist finance, Wesseling took the available information into consideration and analysed the Agreement only as an investigation tool for terrorist attacks, not as a preventive tool for stopping those attacks from happening, unlike the considerations made in favour of its conclusion in the first place.[150] The necessity of the TFTP-II is, therefore, debatable.

The next step on assessing the proportionality of the TFTP-II is to determine the amount of data to be transferred and the relation of this data to public security. Article 4 of the Agreement sheds light on the manner in which the requests from the US to obtain Europe-originating data are required to be 'tailored as narrowly as possible.'[151] Having this in mind, as was stated in the Commission's Communication of July 2011, the financial data has been provided in bulk due to the fact that it was not technically possible to provide data on an individual basis.[152] This enables the US to gain data related to citizens who are not the object of any suspicion.[153] Although this communication was made in 2011, more recently in

[145] ibid, para 45.
[146] ibid, para 46 (Emphasis added).
[147] Digital Rights Ireland CJEU (n 2), para 49.
[148] ibid.
[149] European Commission, Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of Terrorist Tracking Program, SWD(2012)454 final, (Brussels, 14 October 2012) 5.
[150] Wesseling and Goede (n 43), 28.
[151] The 2012 PNR Agreement (n 73), Article 4.
[152] European Commission, 'Communication on a European terrorist finance tracking system: available options' (n 41), 2-3.
[153] ibid.

2013 Europol's Joint Supervisory Body reaffirmed this fact and observed this mass data transfer as being 'unchanged.'[154] However, in *Digital Rights Ireland* the CJEU demanded the need to demonstrate the link between the data and the threat to public security.[155] Unfortunately, the TFTP-II falls short of providing this link as it allows bulk transfer of financial data to a third country.[156]

As for the storage of the financial data transferred to the US, the TFTP-II requires a maximum period and it ensures that the data shall be erased when it is no longer necessary to combat terrorism or its financing.[157] Here, the definition of 'non-extracted data' required by Article 6 necessitates further attention. In the EDPS's opinion this definition is vague.[158] If one assumes that this definition relates to data that has been stored due to bulk transfer, but has not been accessed or used for a specific investigation, the 5 year storage period for such data transferred irrespective of nexus to terrorism should be considered as excessive.[159]

Moreover, in assessing whether a restrictive measure is proportionate the CJEU demands the access made by law enforcement authorities to be reviewed by 'a court or by an independent administrative body.'[160] By way of this review and the decision made thereof, the access to data and its use can be ensured to be limited 'to what is strictly for the purpose of attaining the objective pursued.'[161] The establishment of an independent authority is also required under Article 8(3) of the Charter in order to review whether the personal data is processed in accordance with the EU data protection principles.

Under the TFTP-II, the requests from the UST for the transfer of EU-originated data are directed to Europol.[162] Europol then reviews these requests in order to confirm that they are in compliance with the TFTP-II requirements.[163] It is questionable whether giving this review task to Europol is appropriate. Article 10 gives Europol power to request relevant US TFTP-originated information if it has a reason to believe that a person or an entity has a nexus to terrorism.[164] Therefore, as the EDPS pointed out, this power might require having good relations with the UST and this in turn calls the independence of Europol, regarding its monitoring task, into question.[165] Another argument contra to Europol's review task is, as Amicelle argued, Europol as a law enforcement body, rather than a judicial one, would review the US requests from a security perspective and would fall short on reviewing these requests for their legality.[166]

The TFTP-II also lays down some rights conferred to data subjects such as the right to be informed (Article 14), right to access (Article 15), right to rectification, erasure or blocking (Article 16) and right to redress (Article 18).[167] The question as to the enforceability

---

[154] Joint Supervisory Body of Europol, 'Implementation of the TFTP Agreement: assessment of the follow-up of the JSP recommendations' (Brussels, 18 May 2013) <http://europoljsb.consilium.europa.eu/media/250972/13-01%20report%20art%204%20tftp%20inspection%202012.pdf> (accessed on 26 April 2016).

[155] Digital Rights Ireland CJEU (n 2), para 59.

[156] See generally Boehm and Cole (n 95), 74.

[157] The 2012 PNR Agreement (n 73), Article 6.

[158] EDPS, 'Opinion on the TFTP-II' (n 29), 5.

[159] ibid.

[160] Digital Rights Ireland CJEU (n 2), para 62.

[161] ibid.

[162] The TFTP-II (n 30), Article 4(3).

[163] ibid, Article 4(5).

[164] The 2007 PNR Agreement (n 65), Article 10.

[165] EDPS, 'Opinion on TFTP-II' (n 29), 6.

[166] Amicelle (n 19), 11; See also Boehm and Cole (n 95), 74.

[167] According to the case-law of the ECtHR and CJEU safeguards against the risk of abuse and of unlawful access and use of data need to be provided if a measure pertaining to limitations on the exercise of the right to privacy and data protection is found to be lawfully permissible. See Weber and

of these rights remains unsettled.[168] As an example, the circumstances limiting the disclosure of data include the purpose of preventing terrorism, among others.[169] Since this security exception was introduced by states, it may well be used as an excuse for mass surveillance of individuals.

Data mining or automated profiling is prohibited under the TFTP-II.[170] This prohibition can be invoked in relation to the use of Big Data practices. Nevertheless, the bulk transfer of data with an ambiguous purpose and the lack of independent oversight mechanisms along with unenforceable data subject's rights makes the Agreement incapable of responding to concerns over the possibility of such use.

In light of the above, it is unconvincing that the financial data transfer required by the TFTP-II is consistent with the proportionality and necessity principles. Given the criteria set out for the data retention measures in the CJEU's recent decision of *Digital Rights Ireland* and the importance of the Charter, the Agreement falls short of ensuring the respect for EU citizens' fundamental rights.

EU-US Passenger Name Record Agreement

Identical issues must be considered in respect of the legality test for TFTP-II. Two main points must be taken into account in order to justify the surveillance measures as required by the 2012 PNR Agreement: are these measures within the limits of what is appropriate, and are they necessary to achieve the purpose of the Agreement? If one can answer both questions in the affirmative, then these restrictive measures can be justified.

Before further discussing the issue it is important to note here that following the 2007 PNR Agreement, the EU also concluded agreements for the transfer of PNR data with Canada and Australia. After the *Digital Rights Ireland* decision, the EU Parliament referred the EU-Canada PNR Agreement to the CJEU for its opinion on the compatibility of this agreement with the EU Treaties and the Charter.[171] Like the 2012 PNR Agreement, this PNR Agreement also enables mass collection of EU citizens' personal data. However, the EU-Canada PNR Agreement differs from the one concluded with the US as to the data surveillance requirements. For example, the EU-Canada PNR Agreement requires a lesser data retention period when compared to the one concluded with the US.[172] Although more privacy intrusive than its Canadian peer, no such referral has been made so far for the 2012 PNR Agreement.

The purpose of processing PNR by the US created a controversy on the proportionality of the 2012 PNR Agreement. As may be recalled, the PNR shall be used by

---

Saravia v. Germany, App no 54934/00 (ECtHR 29 June 2006) para 106; Digital Rights Ireland CJEU (n 2), para 66.

[168] EDPS, 'Opinion on TFTP-II' (n 29) 6-7; Boehm and Cole (n 95), 75; Murphy (n 14), 157.

[169] The TFTP-II, Article 15(2).

[170] ibid, Article 5(3).

[171] European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice' Press Release (25 November 2014) <http://www.europarl.europa.eu/news/en/news-room/content/20141121IPR79818/html/MEPs-refer-EU-Canada-air-passenger-data-deal-to-the-EU-Court-of-Justice> (accessed on 26 April 2016).

[172] There are two data retention periods under the EU-Canada PNR Agreement. Mostly, the data is retained for 3.5 years. The data relating to a person who is subject of an investigation in Canada is retained for a maximum of 6 years. See Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, 2006/253/EC, OJ L 91/46 (29 March 2006). When comparing the US PNR scheme with the ones concluded with Canada and Australia, Murphy emphasizes the variety of data retention periods under every PNR agreement concluded with the EU and states that this variance may suggest that those PNR agreements and their conditions depend on political negotiations, not on an objective assessment as to the compliance of these agreements with the necessity and proportionality principles. See Murphy (n 14), 159.

the US 'for the purposes of preventing, detecting, investigating and prosecuting (a) terrorist offences and related crimes and (b) crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature.'[173] Here, the EDPS and Working Party shared the same views as to the uncertainty caused by this provision.[174] For example, the Agreement allows use of the PNR data on 'a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.'[175] This statement is troubling since it makes it possible to use the PNR data even for minor crimes and for non-criminal actions, if ordered by a court.[176] Additionally, 'the transnational serious crime' as provided under Article 4 not only covers law enforcement in the US, but also crimes that are committed in more than one jurisdiction.[177] Departing from these examples, it is evident that the definitions of the limits of using the PNR are not clearly defined.[178] It is worth noting here that in *Digital Rights Ireland*, the CJEU held that for an interference with data protection to meet with the necessity principle, 'the EU legislation must lay down clear and precise rules governing the scope and application of the measures in question.'[179] Unfortunately, the 2012 PNR Agreement lacks clear and precise rules as to the way transferred PNR data should be used by the DHS.[180]

Consideration also should be taken of the data retention period provided by the 2012 PNR Agreement. It is worth noting that despite the EU Parliament's call for a limited data retention period,[181] the Agreement allows data retention of all European passengers, regardless of their criminal background, for up to 15 years. As highlighted by the Working Party, a data retention period this long is excessive and disproportionate.[182] On top of that, the Working Party observed that the Agreement only requires the anonymisation of the data after 15 years, not its deletion.[183] This in turn raises the question of the reasons behind keeping the data further, even if it is anonymised.[184] Moreover, the extensive 15 year retention period is required not only for suspects, but for people on whom no suspicion has fallen as well. This contradicts the CJEU's stand on making a distinction between data categories on the basis of the objective pursued or according to persons concerned.[185] Otherwise, treating suspicious and non-suspicious people in the same manner runs the risk of stigmatisation of the former.[186]

---

[173] The 2012 PNR Agreement (n 73), Article 4(1).

[174] Article 29 Data Protection Working Party, 'Open Letter to Members of the LIBE Committee of the European Parliament' (n 72); EDPS, 'Opinion on the 2012 PNR Agreement' (n 72) 4.

[175] The 2012 PNR Agreement (n 73), Article 4(2).

[176] Article 29 Data Protection Working Party, 'Open Letter to Members of the LIBE Committee of the European Parliament' (n 72).

[177] ibid.

[178] 'The Agreement leaves plenty of room for the use of PNR that is linked neither to fighting terrorism nor serious crime, hence leaving its purpose open to variety of other uses.' See Boehm and Cole (n 95), 59-60.

[179] Digital Rights Ireland (n 2), para 54.

[180] See, Article 29 Data Protection Working Party, 'Open Letter to Members of the LIBE Committee of the European Parliament' (n 72).

[181] European Parliament, 'Resolution of 5 May 2010' (n 82).

[182] Article 29 Data Protection Working Party, 'Open Letter to Members of the LIBE Committee of the European Parliament' (n 72).

[183] ibid.

[184] ibid. Here, Boehm and Cole argue that the reason behind retaining anonymised data for an indefinite term is to re-personalise such data when needed during this term. The authors further argue that if the re-personalisation of anonymised data seems possible, then the terms in Article 8 of the 2012 PNR Agreement, such as anonymization must be defined clearly. See Boehm and Cole (n 95), 61.

[185] Digital Rights Ireland CJEU (n 2), para 63.

[186] See Boehm and Cole (n 95), 61. See also; S and Marper v. UK App nos 30562/04 and 30566/04 (ECtHR 4 December 2008) para 112.

As for the amount of data to be collected and subsequently sent to the US, the 2012 PNR Agreement lists nineteen types of data.[187] Given the fact that the same list of data contained in the 2007 PNR Agreement was already considered as inconsistent with the proportionality principle,[188] the same conclusion can be drawn for the 2012 PNR Agreement. Additionally, the required list contains sensitive data about the passengers, such as their religious belief or health.[189] Could the processing of this sensitive data have subsequent discriminatory impact on the passenger? This can only be forestalled if the Agreement explicitly prevents data mining and profiling. Despite the EU Parliament's call for limiting the use of PNR data to a case-by-case basis and not allowing without exception this data to be used for data mining or profiling,[190] a mere reading of the 2012 PNR Agreement shows that it does not contain any prohibition as such. Recalling here Big Data practices, the Agreement by way of entailing a possible risk of profiling on all passengers aggravates the negative impacts of data processing measures on individuals' fundamental rights.

The CJEU consistently mentioned providing sufficient guarantees to individuals to effectively protect their personal data against risk of abuse and against any unlawful access and use.[191] Returning to the 2012 PNR Agreement, individuals are given the possibility to seek administrative and judicial redress in accordance with US law.[192] Therefore, it is evident that specific knowledge of US law is sufficient and it is not clear whether those redress mechanisms will be effective in practice.[193]

Taking all these matters into account, the proportionality of the measures required by the 2012 PNR Agreement for countering terrorism remain unsettled. A reference to *Digital Rights Ireland* again sheds light on the current debate. In this decision the retention of communications data of all European citizens was found to 'entail a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU.'[194] The same conclusion can be drawn for the 2012 PNR Agreement because it allows for a systematic bulk transfer of data about all persons, in spite of the absence of any link between them and terrorism threats. Consequently, the PNR 2012 Agreement fails to comply with the proportionality requirements of the Charter and the case-law of the CJEU.

5. Conclusion

Terrorist Finance Tracking and EU-US Passenger Name Records Agreements provide data transfers to US law enforcement authorities for the prevention, investigation, detection or prosecution of terrorism. The arguments in support of these Agreements have always revolved around their usefulness for countering terrorism and they have been regarded as valuable tools thereof. However, an assessment of their usefulness is not sufficient to prove these agreements are lawful. It is evident that both agreements represent a massive collection and use of personal data about European citizens. From there, at least from an EU perspective, both Terrorist Finance Tracking and EU-US Passenger Name Records Agreements need to be assessed in line with fundamental rights laid down under the Charter

[187] The 2012 PNR Agreement (n 73), Annex.
[188] Article 29 of the Data Protection Working Part, Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in 2007, 01646/07/EN WP 138 (17 August 2007) 11.
[189] EDPS, 'Opinion on the 2012 PNR Agreement' (n 72), 5.
[190] European Parliament, 'Resolution of 5 May 2010' (n 82).
[191] Digital Rights Ireland CJEU (n 2), para 54.
[192] The 2012 PNR Agreement (n 73), Article 14(1).
[193] Article 29 Data Protection Working Party, 'Open Letter to Members of the LIBE Committee of the European Parliament' (n 72); Boehm and Cole (n 95), 65.
[194] Digital Rights Ireland CJEU (n 2), para 65.

of Fundamental Rights, more specifically in line with the right to privacy and personal data protection, in order to be justified.

According to the Charter and the jurisprudence of the CJEU, public security does not grant an unlimited discretion for derogating and limiting fundamental rights of European citizens. Therefore, restrictive measures on the right to privacy and personal data protection employed for countering terrorism must not undermine these rights. In this regard, any interference with European citizens' fundamental rights must be justified in each case. Do the Terrorist Finance Tracking and EU-US Passenger Name Records Agreements extend the limit of what is strictly necessary and proportionate in light of their objective of combating terrorism? An in depth look at these agreements shows that they constitute data retention measures about all people, regardless of whether they are suspected or not of terrorist related activities. In other words, they require a systematic and disproportionate retention and transfer of data. To this end, they exceed the limits of what is necessary and proportionate as imposed by the Charter in respect of the right to privacy and personal data protection.

After finding the Terrorist Finance Tracking and EU-US Passenger Name Records Agreements not in compliance with the right to privacy and personal data protection, the question remains as to the future of these agreements. Given the growing importance of the Charter and the recent decision of the CJEU in which the data retention measures imposed by the Data Retention Directive were found to be of a disproportionate nature and therefore in breach of fundamental rights, it is possible that the Terrorist Finance Tracking and EU-US Passenger Name Records Agreements will be found invalid if they are challenged before the CJEU. In this regard, the necessity and proportionality of the agreements at stake must be reconsidered in line with the Charter and the settled case-law of the CJEU.