the SPANISH YEARBOOK of INTERNATIONAL LAW

Flying from the EU to the US: necessary extraterritorial legal diffusion in the US-EU Passenger Name Record agreement

Mistale TAYLOR*

Abstract: The US-EU Passenger Name Record (PNR) agreement provides guidance on processing and transferring EU citizens' airline passenger data to the US Department of Homeland Security for counterterrorism and security purposes. The US and the EU have struggled to conclude an agreement that satisfies all their concerns. Different conceptual approaches to security and counterterrorism, and privacy and data protection, have rendered the bilateral negotiations particularly onerous. To better safeguard the fundamental right to data protection for EU citizens, EU authorities should push for the PNR agreement to incorporate more EU data protection standards, especially in view of recent Court of Justice of the European Union developments. If incorporated into the agreement, this could be seen as a necessary form of legal diffusion of EU data protection standards beyond its borders.

Keywords: data protection - EU law – extraterritoriality – PNR agreement

INTRODUCTION

After more than a decade of cumbersome negotiation, three versions and one annulment, the current US-EU Passenger Name Record (PNR) agreement, from 2011, still does not satisfy EU data protection concerns. The agreement establishes a set of guidelines on processing and transferring EU citizens' airline passenger data to the US Department of Homeland Security (DHS), largely for counterterrorism purposes.[1] Conceptual approaches to security, counterterrorism, privacy and data protection on both sides of the Atlantic are divergent, but fluid. As such, the parties have found it difficult to conclude an agreement that satisfies all their concerns. The current PNR agreement from 2011 is undergoing review.

Data protection is a fundamental right in the EU, and in view of the May 2014 *Digital Rights Ireland* judgement and the November 2014 referral of the Canada-EU PNR agreement to the CJEU, it is becoming increasingly apparent that the current US-EU PNR agreement does not live up to EU

* PhD candidate at Utrecht University and Senior Research Associate at Public International Law and Policy Group. Thank-you to Professor Cedric Ryngaert and Professor John Vervaele for comments on an earlier draft. The research that resulted in this publication was funded by the Dutch Organization for Scientific Research under the VIDI Scheme. This publication also forms part of the RENFORCE/CLEER project on The External Effects of European Union Law. All websites accessed 16 November 2015.

[1] Council of the European Union, 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, 8 December, 2011; the 2004 PNR agreement refers to the Department of Homeland Security Bureau of Customs and Border Protection (CBP), but the present uses DHS to cover the CBP, too.

 DOI: 10.17103/sybil.19.14

data protection standards.[2] This leads to the questions of how precisely the agreement fails to uphold EU data protection principles; how these failures could be rectified; and how this rectification would imply a degree of extraterritoriality.

To better safeguard the fundamental right to data protection for EU citizens, in negotiations with the US, EU authorities should push for the PNR agreement to incorporate more EU data protection standards. If incorporated into the agreement, this could be seen as a necessary form of legal diffusion beyond its borders as the DHS processes EU citizens' data on US soil. Indeed, in light of recent legal developments, EU data protection principles could necessarily extend beyond EU territory in the PNR context. The following briefly outlines the evolution of the US-EU PNR agreements and then examines how the agreements adhere to data protection principles espoused in the Data Protection Directive (DPD) and the recent *Digital Rights Ireland* judgement, highlighting how the agreement could and should better protect EU citizens' fundamental right to data protection. This scope for improvement lends itself to a soft form of the extraterritorial application of EU law.

THE US-EU PNR AGREEMENT NEGOTIATIONS AND VALUE-BASED TENSIONS

The DHS began collecting passenger information in response to the 2001 terrorist attacks in the US.[3] The US-EU PNR agreement aims to counteract terrorism and serious transnational crime. Any passenger flying between the EU and US must have his or her personal data recorded and stored for security purposes.[4] Examples of PNR data types include passenger names and contact details, booking and travel dates, and all available payment information. Whilst the European Commission's agenda in concluding the agreement initially focused on maintaining the transatlantic air transport market, other stakeholders, such as the Article 29 Data Protection Working Party, quickly highlighted potential privacy issues with the PNR agreement.[5] The Article 29 Working Party, which consists of Member State Data Protection Authority representatives, the European Data Protection Supervisor and European Commission representatives, offers recommendations and opinions on EU data protection law. More than a decade of negotiations and revised PNR agreements highlights the difficulties the EU and US have had in concluding an agreement that sufficiently satisfies the EU's data protection interests and the US' security interests.

---

[2] CJEU, Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others*, Joined cases C-293/12 and C-594/12; European Parliament, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice', press release, 25 November 2014 *text available at* 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; E. Masse, 'Wishing "Bon voyage" to PNR agreements in Europe', accessnow.org, 26 November 2014 *text available at* https://www.accessnow.org/blog/2014/11/26/wishing-bon-voyage-to-pnr-agreements-in-europe.

[3] European Commission, 'Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records in the United States Department of Homeland Security', {COM(2013) 844 final}, 27.11.2013, SEC(2013) 630 final, 2013.

[4] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data in the United States Department of Homeland Security (DHS), 2007.

[5] A. Newman, 'Transatlantic Flight Fights: Multi-level governance, actor entrepreneurship and international anti-terrorism cooperation', 18(4) *Review of International Political Economy* (2011) 481-505, at 490-491.

 DOI: 10.17103/sybil.19.14

In general, a controller, that is, an airline carrier, located in an EU Member State collects PNR data. As such, the relevant State's national laws, pursuant to the EU's DPD, apply to the data processing.[6] According to the DPD, when transferring personal data to third States where the data will be processed, the third State must ensure an adequate level of data protection.[7] The EU does not consider the US to satisfy the adequacy requirements of the Directive, rendering any PNR data transfers to the US unlawful under the Directive per se. In contrast, US law obliges airlines to transfer PNR data to the US. As such, this conflict of laws warranted bilateral negotiations, the evolution of which is explored below.[8]

THE EVOLUTION OF THE PNR AGREEMENTS

The US-EU negotiations and the evolution of the 2004, 2007 and 2011 PNR agreements show how the two parties have tried, successfully and unsuccessfully, to apply their value-based laws to EU citizens' personal data. Despite the EU's continual attempts to ensure an EU level of data protection when that data is transferred to the US, the US has resisted these attempts at such diffusion of EU law beyond its borders.

The *de jure* situation, however, reads differently. The 2011 PNR agreement refers to values supposedly common to the US and EU. For instance, the agreement affirms both parties desire "to prevent and combat terrorism and serious transnational crime effectively [to protect their] common values", "while respecting fundamental rights and freedoms and recognising the importance of privacy and the protection of personal data and information".[9] Indeed, these references suggest the two parties agree on how much weight ought to be accorded to the values of security and data protection, and then translated into legislation.

The reality, however, as gleaned from the myriad negotiations, joint reviews, and US and EU political and civil society reactions, shows a long-lived struggle between the parties to protect their own competing interests and implied jurisdictional claims. It is difficult to say whether the current PNR agreement reflects an extension of the "long arm" of EU data protection law or a regurgitation of US demands.[10]

(1) The 2004 Agreement

---

6 Commission Directive 95/46 (DPD), OJ 1995 L 281, Art. 4(1).

7 *Ibid*., Art. 25; "[T]he transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited" – *Ibid*., recital 57.

8 *Ibid*., Art. 25(6); G. Hornung and F. Boehm, 'Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security', 14 March 2012, at 5.

9 2011 PNR agreement, *supra* n. 1, preamble; more specifically, one of the main EU complaints about the PNR is its violation of the proportionality and necessity principles, however the agreement's preamble states: "the United States and the European Union [recognize] the related principles of proportionality as well as relevance and necessity that guide this Agreement and its implementation by the European Union and the United States" – *Ibid*..

10 L. Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to the Processing of Personal Data of EU Citizens by Websites Worldwide?', 1(1) *International Data Privacy Law* (2011), 28-46.

 DOI: 10.17103/sybil.19.14

In a speedy reaction to the September 11 attacks on the US, in November 2001, the US government enacted and instituted the Aviation and Transportation Security Act of 2001 (Act or PNR Act), obliging air carriers to give US customs electronic access to PNR data on those passengers entering or leaving the US.[11] In June 2002, the European Commission informed the US that the Act's requirements could conflict with EU and Member State legislation.[12] The two parties accordingly began negotiations. Whilst US officials postponed the entry into force of the Act's new provisions, they "refused to waive the right to impose penalties on airlines failing to comply with the legislation on electronic access to PNR data after 5 March 2003".[13] This resulted in many EU Member State airlines allowing US customs access to their PNR data.[14] Whilst the US agreed to negotiate with the EU on the data protection provisions of its PNR Act, it enforced penalties on non-compliant EU air carriers. The effect of this was such that US authorities would still collect and store PNR data from EU carriers, thereby protecting their national security interests, but disregarding EU data protection standards. Acknowledging the importance of countering terrorism, it was important to solve this issue to protect EU citizens' personal data and to address the legal uncertainty many air carriers faced.[15] In 2004, the two parties concluded the first PNR agreement.

In May 2006, the CJEU annulled the Council Decision on the conclusion of the US-EU PNR agreement, ruling that it was concluded *ultra vires*; it did not make pronouncements on whether the agreement violated the rights to privacy and/or data protection.[16]

(2) The 2007 and 2011 Agreements

In 2007, the US and EU concluded a new PNR agreement, which applied only provisionally due to the Parliament's continued concerns with its lack of privacy and data protection safeguards.[17] As the US government believed it was improbable the European Parliament would approve the 2007 version of the PNR agreement, they agreed, warily, to reopen PNR agreement negotiations.[18] In December 2011 and April 2012, the European Council and Parliament respectively approved the revised version of the agreement.[19]

(3) The Current Situation

Whilst the two parties' value-conceptions are rooted in history, they evidently evolve according to present-day concerns. In late 2014, the European Parliament's Civil Liberties, Justice and Home

[11] Aviation and Transportation Security Act of 2001, Public Law 107–71—Nov. 19, 2001 (codified at 49 U.S.C. 44909(c)(3)).

[12] European Commission, 'Joint Review' *supra* n. 3, at 2.

[13] CJEU, Judgment of the Court (Grand Chamber) of 30 May 2006, *European Parliament v Council of the European Union and European Parliament v Commission of the European Communities*, Joined cases C-317/04 and C-318/04, §33.

[14] *Ibid.*, §33.

[15] *Ibid.*, §44.

[16] *Ibid.*, §§69-70.

[17] 2007 PNR agreement, *supra* n. 4.

[18] K. Archick, Congressional Research Service, 'U.S.-EU Cooperation Against Terrorism', December 1 2014, at 18.

[19] Council Decision of 13 December 2011 2012/381, OJ 2012 L 186; 'MEPs back deal to give air passenger data to US', *BBC News*, 19 April 2012.

 DOI: 10.17103/sybil.19.14

Affairs (LIBE) Committee acknowledged that the EU was more vulnerable to security threats than one year previously.[20] This did not have an immediate impact on the question of data protection, although it will be interesting to see how the CJEU in assessing the Canada-EU PNR agreement weighs up the two concerns. Since then, 2015 terrorist attacks in Paris have ignited general EU security debates, whilst the 2014 *Digital Rights Ireland* decision shows a return to stricter data protection laws, both of which have ramifications for the US-EU PNR agreement. Despite a potential move in the EU to laws that foreground security interests in the way comparable to the Data Retention Directive (DRD), the Union has an enduring commitment to data protection. Accordingly, the "popular narrative of an imperial security oriented US government bullying a human rights focused European government into submission" is somewhat reflected in the PNR agreement negotiations.[21]

EU DATA PROTECTION PRINCIPLES AND THE PNR AGREEMENTS

The EU's data protection principles are articulated in the DPD and include purpose limitation; third party access to data, including onward transfers; data retention; data types, including sensitive data; and judicial redress.[22] In view of the May 2014 *Digital Rights Ireland* judgement, the October 2015 *Schrems* judgement and the November 2014 referral of the Canada-EU PNR agreement to the CJEU, the following looks at EU data protection principles as outlined in the DPD and shows how the US-EU PNR agreement fails to adhere to them. Acknowledging this failure and incorporating these principles into the next data sharing agreement would result in EU data protection law principles extending beyond its territorial boundaries.

The following focuses closely on the *Digital Rights Ireland* decision as it is more directly connected with the PNR agreement. It is, however, necessary to mention the CJEU's 6 October 2015 ruling in the *Schrems* case, which concerned the transfer of EU citizens' to the US under the bilateral Safe Harbour agreement and associated concerns of mass surveillance by US authorities, and which will undoubtedly influence future PNR agreement dialogues.[23] In that case, the Court declared the Safe Harbour agreement invalid for several reasons. The main reason was that the agreement did not prevent US authorities from interfering with EU citizens' fundamental right to data protection, especially as US security and law enforcement requirements overrule protections in the Safe Harbour agreement.[24] The European Parliament has since urged the Commission to assess the decision's impact on, inter alia, the PNR agreement.[25]

---

[20] European Parliament, LIBE Committee press release, 'MEPs debate plans to use EU Passenger Name Record (PNR) data to fight terrorism', 11 November 2014 *text available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20141110IPR78121%2bo%2bDOC%2bXML%2bV0%2f%2fEN&language=EN.

[21] Newman, *supra* n. 5, at 485 *cit.* J. Klosek, *The War on Privacy* (Praeger Publishers, Westport, 2007).

[22] See DPD, *supra* n. 6, Art. 6.

[23] CJEU, Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14.

[24] *Ibid.*, §§86 and 98.

[25] EP resolution of 29 October 2015, 2015/2635(RSP), §19.

A November 2010 European Parliament resolution on a global approach to PNR agreements, including those with Australia and Canada, summarized the general collective EU stance regarding the US PNR agreement, particularly in light of the importance of protecting what is enshrined in the EU Charter on Fundamental Rights (EU Charter) as a discrete, fundamental right to data protection. The Parliament emphasized that the legal basis of any PNR agreement must include Article 16 of the Treaty on the Functioning of the European Union (TFEU) on the right to data protection.[26] The legal bases for all three EU-third State PNR agreements have failed to include Article 16 (TFEU). The Parliament also highlighted the importance of the proportionality and necessity principles, which most commentators complained the US-EU PNR agreement violated.[27] Below some more specific principles are outlined.

(1) Purpose Limitation

The DPD provides that personal data must be collected for "specified, explicit and legitimate purposes" and the data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".[28] The uses for personal data as articulated by the 2004, 2007 and 2011 PNR agreements have increased demonstrably over the years. Moreover, it is unclear how the 2007 and 2011 agreements relate uniquely to their stated goals of counteracting terrorism, and serious and organised crime.[29] The 2004 agreement, for instance, limited the data use to preventing and combating terrorism and related crimes, and other serious transnational crimes, including organized crime.[30] The 2011 agreement uses data for, inter alia, "the purposes of preventing, detecting, investigating, and prosecuting terrorist offences and related crimes, including [...] conduct that [...] appears to be intended to intimidate or coerce a civilian population".[31] Whilst that agreement appears more specific than the 2004 one, it construes the data use so broadly and vaguely, that its purpose limitation clauses evidently do not comply with EU data protection standards as set out in the DPD.[32]

---

[26] EP resolution of 11 November 2010, P7_TA-PROV(2010)0397, §5. See also, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01, Art. 16 *text available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=en.

[27] *Ibid.* (EP resolution).

[28] DPD, *supra* n. 6, Art. 6(1)(b) and (c).

[29] On purpose limitation, "As a consequence, the mentioned purposes are not specifically linked to the overarching goal of the prevention, detection and investigation and prosecution of terrorist and related crime, which were subject to the former agreements. PNR data can be thus used for other purposes not related to terrorist or serious crimes (i.e. border control, use if ordered by a court, other violations of law)" – Hornung and Boehm, *supra* n. 8, at 7.

[30] European Commission, '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', CE/USA/en 1, 2004, *cit.* UNDERTAKINGS OF THE DEPARTMENT OF HOMELAND SECURITY BUREAU OF CUSTOMS AND BORDER PROTECTION (CBP), 11 May 2004 *text available at*http://www.statewatch.org/news/2006/jun/US-EUa-pnr-undertakings-may-2004.pdf, Art. 3.

[31] 2011 PNR agreement, Art. 1(a).

[32] F. Boehm and M. Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union', 30 June 2014 *text available at* http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf, p. 66.

This observation contrasts starkly with the 2011 US Senate resolution, acknowledging a 2010 US-EU joint review of the PNR agreement, that found the DHS' collection of PNR data had not led to privacy violations, misuse or injury, and reaffirmed that both the US and EU governments were committed to data protection and respecting individual privacy.[33] The same resolution asserted the PNR agreement complied with both parties' privacy laws, "by providing assurances that the United States would use PNR data for limited purposes".[34] This assertion conflicts with EU issues with the lack of purpose limitation in the PNR agreement. The Senate also claimed PNR data had been used successfully to identify and arrest terrorists.[35] It is unclear, however, how PNR data transfer has achieved its stated goals and how its expanded use over the years has translated into a more effective achievement of its aims.[36]

The CJEU's jurisprudence confirms that the proportionality principle "requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives".[37] The legitimate objectives the European Parliament and Council aimed to achieve with the DRD were to harmonize Member State laws on retaining telecommunications data to detect, investigate and prosecute serious criminals.[38] This recalls the aims of the 2011 US-EU PNR agreement.[39]

(2) Data Retention

The DPD and recent jurisprudence outline limitations on retaining personal data. The CJEU's decision in the landmark 2014 *Digital Rights Ireland* case could have tangible ramifications for the US-EU PNR agreement. In that judgement, the CJEU annulled the DRD.[40] The Court ruled that the 2006 DRD, which obliged Member States to retain EU citizens' telecommunications data for between six months and two years to help fight serious crime and terrorism, violated the principles of proportionality and necessity.[41] Moreover, the Court stated the DRDcaused a"wide-ranging" and "particularly serious" interference with fundamental rights.[42] As the Directive did not outline clear and precise rules on the limits of the interference with the fundamental rights to privacy and data protection, thereby violating the principle of necessity, it constituted an extremely serious

---

33 Archick, *supra* n. 18, at 18.

34 *Ibid.*

35 S.Res. 174, 112th Congress, (18 May, 2011) available at https://www.govtrack.us/congress/bills/112/sres174/text.

36 Hornung and Boehm, *supra* n. 8, at 7.

37 *Digital Rights Ireland*, *supra* n. 2, §46 *cit.* CJEU, Case C-343/09 *Afton Chemical* EU:C:2010:419, §45; *Volker und Markus Schecke and Eifert* EU:C:2010:662, §74; Cases C-581/10 and C-629/10 *Nelson and Others* EU:C:2012:657, § 71; Case C-283/11 *Sky Österreich* EU:C:2013:28, §50; and Case C-101/12 *Schaible* EU:C:2013:661, §29.

38 Commission Directive 06/24 (DRD), OJ 2006 L 105, Art. 1(1).

39 2011 PNR agreement, *supra* n. 1, at preamble.

40 *Digital Rights Ireland*, *supra* n. 2, §73.

41 DPD, *supra* n. 39; *Digital Rights Ireland*, *supra* n. 2, §§65 and 69.

42 *Digital Rights Ireland*, *supra* n. 2, §37.

interference with those rights.[43] The PNR agreement also fails to set out specific rules limiting the interference with the right to data protection.

The CJEU pronounced that, by adopting the Directive, the EU legislature failed to act in accordance with the proportionality principle.[44] The Court thus declared the Directive invalid.[45] In light of this, it can be asked whether the US-PNR agreement's 15 year retention period could be affected by the judgement. If so, changing the agreement to accommodate the CJEU's ruling could be a form of the EU extending the reach of its changed laws. The decision is helpful to evaluate the legality of the PNR agreement, but as it is limited to a discussion on data retention, and the PNR is broader in scope than the Directive, it would not provide a definitive answer on the legality of the PNR agreement.

Any limit on the enjoyment of a right or freedom under the EU Charter must be provided for by law; respect the essence of the right or freedom concerned; and, particularly relevant to data retention, must be subject to the principle of proportionality: "limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others".[46] In 2006, the CJEU annulled the 2004 PNR agreement as it was not concluded on an appropriate legal basis, so it is not unfathomable that the Court would have to consider the legality of the 2011 PNR agreement in the future. It is also plausible that the PNR agreement needs to be renegotiated following the CJEU's finding the DRDinvalid. In November 2014, for instance, the European Parliament voted with a large majority to submit the Canada-EU PNR agreement, concluded on the same legal basis as the US-EU PNR accord, to the CJEU to assess its compliance with EU treaties and the EU Charter.[47] The *Digital Rights Ireland* decision influenced this referral. A leaked copy of the European Parliament's legal services opinion on the consequences of the CJEU's judgement in the *Digital Rights Ireland* case confirms that EU-third State accords involving personal data will have to be re-evaluated according to the principles of proportionality and necessity evoked in the judgement.[48] Since the judgement, the Commission has consistently iterated that data retention laws are a national concern and that it will not enter that discussion.[49] The effects of the *Digital Rights Ireland* and *Schrems* cases should be evident in the outcome of the next joint review of the PNR agreement, which, as it was originally scheduled for early 2015, should happen in the foreseeable future.

---

[43] *Ibid.*, §65.

[44] *Ibid.*, §69.

[45] *Ibid.*, §71.

[46] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02 *text available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf, Art. 52(1).

[47] European Parliament press release, *supra* n. 2.

[48] D. Naranjo, 'Legal Service Opinion on CJEU Data Retention Ruling', *European Digital Rights (EDRi.org)*, 14 January 2015 *text available at* https://edri.org/legal-service-opinion-on-cjeu-data-retention-ruling/*cit.* European Parliament Opinion on the Court of Justice of the EU's ruling on the Data Retention Directive, 7 January 2015 *text available at* https://s3.amazonaws.com/access.3cdn.net/27bd1765fade54d896_l2m6i61fe.pdf.

[49] European Commission statement on national data retention laws, Brussels, 16 September 2015 *text available at* http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm.

The DPD states that personal data must not be kept in a form allowing for identification of data subjects for longer than necessary for the purposes for which the data was collected and processed.[50] This implies that data can lawfully be stored for an indefinite period if it is anonymized. Further, the 2002 ePrivacy Directive, as referenced by the CJEU in *Digital Rights Ireland*, provides that Member States shall ensure storing data or accessing stored data "is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing".[51]

The ePrivacy Directive also states Member States may adopt legislation that restricts the rights and obligations in that Directive, which largely revolve around protecting personal data, "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security".[52] The DRD provided that retaining data was necessary and effective for law enforcement to investigate organized crime and terrorism in certain Member States and therefore necessitated making data retained under that Directive available to law enforcement.[53] Nonetheless, the CJEU decided this general interest objective, that is, to combat serious crime, organized crime and terrorism, did not per se justify the level of data retention the DRD required.[54] It will be interesting to see how this conclusion could affect the PNR agreement, which has almost identical objectives.

The CJEU took issue with the blanket data retention the DRD required. Operators were obliged to store all clients' personal telecommunications data, not just the data of those who were likely to be involved in a serious crime.[55] The CJEU stated the Directive thus resulted in an "an [unlawful] interference with the fundamental rights of practically the entire European population".[56] According to the PNR agreement, air carriers conducting passenger flights to and from the US and the EU are obliged to transfer 19 types of PNR data from each journey in their reservation systems, pertaining to suspicious and unsuspicious passengers alike, to the DHS.[57] This indiscriminate transfer requirement could conflict with the CJEU's pronouncements on blanket data retention.

The Court ruled that the DRD did not provide for distinction between data types according to potential usefulness; it also failed to outline a way to determine objectively how long personal data should be retained within the data retention period of 6 to 24 months.[58] This violated the principle of necessity insomuch as an indiscriminate volume of anyone's personal data could potentially be retained for a period of time exceeding the limits of what was necessary.[59] The 2011 PNR agreement contains provisions that would allow for data retention that clearly violate the principle of necessity as

50 DPD, *supra* n. 6, Art. 6(1)(e).
51 Commission Directive 02/58 (ePrivacy Directive), OJ 2002 L 201, Art. 5(3).
52 *Digital Rights Ireland*, *supra* n. 2, §10 *cit.* ePrivacy Directive, *ibid.* Art. 15(1), see also Recital 4 of the preamble.
53 DRD, *supra* n. 38, preamble, Recital 9.
54 *Digital Rights Ireland*, *supra* n. 2, §51.
55 *Ibid.*, §37.
56 *Ibid.*, §56.
57 2011 PNR agreement, *supra* n. 1, Art. 3.
58 *Digital Rights Ireland*, *supra* n. 2, §§63-64.
59 *Ibid.*, §§63-64.

the CJEU applied it in the *Digital Rights Ireland* decision. After a period of 5 active years, data is transferred to a non-active or dormant database for up to 10 additional years.[60] The agreement states that after the dormant period, the data must be anonymized, but it makes no mention of deletion.[61] Compare this to the 2007 agreement, in which DHS officials "expect[ed]" PNR data would be deleted after the 15 year retention period.[62] It appears the PNR data of US-EU passengers could be retained, perhaps unnecessarily, for up to 15 years and potentially indefinitely thereafter. There is only one restriction no which type of data may be retained for longer in the active database: data "related to a specific case or investigation may be retained in an active PNR database until the case or investigation is archived".[63] Further, PNR data in the dormant database can be repersonalized "in connection with law enforcement operations and then only in connection with an identifiable case, threat or risk"; dormant PNR data can be repersonalized for up to five years.[64] It is useful to recall the DPD provision that identifiable personal data must not be stored longer than necessary, but anonymized data could, by extension, be retained beyond this necessary period. The 2011 PNR agreement increases the data retention period when compared with the previous agreements, but provided this retention satisfies the proportionality and necessity principles, US storage of anonymized data could be lawful.

(3) Third Party Access to Data

The DPD provides that processing personal data is permitted only if, inter alia, it is necessary for "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party" or "purposes of the legitimate interests" of a third party "except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject".[65] The *Digital Rights Ireland* judgement asserts that obliging telecommunications companies to retain data pertaining to someone's private life per seconstitutes an interference in the right to respect for private and family life as enshrined in the EU Charter.[66] The Court refers to European Court of Human Rights (ECtHR) jurisprudence to reaffirm that granting competent national authorities access to that data is a further interference in this right.[67] This directly contradicts with the PNR agreement's provisions on storing personal data related to someone's private life and allowing national authorities access thereto. Further, the US has expanded the potential for onward transfer under the PNR agreement. According to the 2004 agreement, the US

[60] 2011 PNR agreement, *supra* n. 1, Art. 8(3).
[61] *Ibid.*, Art. 8(4).
[62] 2007 PNR agreement, *supra* n. 4, Art. VII.
[63] 2011 PNR agreement, *supra* n. 1, Art. 8(5).
[64] *Ibid.*, Arts. 8(3) and (4).
[65] DPD, *supra* n. 6, Arts. 7(e) and (f).
[66] *Digital Rights Ireland*, *supra* n. 2, §34.
[67] *Digital Rights Ireland*, *supra* n. 2, §35; Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5 *text available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf, Art. 8; see cases ECtHR, *Leander v. Sweden*, 26 March 1987, Application no. 9248/81, §48; ECtHR, *Rotaru v. Romania [GC]*, 4 May 2000, Application no. 28341/95, §46; ECtHR, *Weber and Saravia v. Germany*, 29 June 2006, Application no. 54934/00, §79.

DHS could share PNR data with other US counter-terrorism or law enforcement agencies. The 2007 agreement expanded this to public security authorities, thereby widening the scope of potential onward data transfers to third parties.[68]

The CJEU maintained that the DRD did not provide for "any objective criterion [or substantive and procedural conditions] by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions".[69] The 2011 PNR agreement is similarly silent on providing criteria and conditions for national authorities' access to the data: access is "restricted to a limited number of specifically authorized officials".[70] The dormant database is "subject to additional controls, including a more restricted number of authorized personnel, as well as a higher level of supervisory approval required before access".[71] The PNR agreement fails to delineate what constitutes a "limited number", a "more restrictive number" and "specifically authorized" officials or personnel and, moreover, who decides upon the definition and scope of these terms. A US Congress document highlighted how fewer authorized personnel would be able to access the data over time, in what could be considered a weak attempt to show the US is limiting third party access to data.[72]

The CJEU was concerned that no court or independent body, upon review, could allow or deny national authorities access to the data retained under the DRD.[73] This review phase would have limited access to that strictly necessary for the Directive's objective to fight serious crime and terrorism.[74] That said, the DRD required that access to the data be defined by Member States' domestic law, and dependent on relevant EU law or public international law provisions, especially the ECHR as interpreted by the ECtHR.[75] This appears to provide for more limited access to the retained data than the PNR agreement, which does not provide for such procedures and conditions of access. The closest example of the PNR limiting access pertains to sensitive data: "[it] may be exclusively accessed using restrictive processes on a case-by-case basis with the approval of a DHS senior manager".[76] Based on CJEU jurisprudence, however, this clause in the PNR agreement would not suffice to justify an interference in the right to privacy, as, to establish such an interference, it is not relevant whether data is sensitive or not.[77]

(4) Data Types

Pursuant to an EU request, the US agreed to narrow the number of data types (for example, name, travel agency and so on) from 34 to 19 in the 2007 agreement.[78] Upon closer inspection, however, this

68 Archick, *supra* n. 18, at 16-17.
69 *Digital Rights Ireland*, *supra* n. 2, §60-61.
70 2011 PNR agreement, *supra* n. 1, Art. 8(1).
71 *Ibid.*, Art. 8(3).
72 Archick, *supra* n. 18, at 18.
73 *Digital Rights Ireland*, *supra* n. 2, §62.
74 *Ibid.*, §62.
75 ePrivacy Directive, *supra* n. 51, Art. 4.
76 2011 PNR agreement, *supra* n. 1, Art. 6(3).
77 *Digital Rights Ireland*, *supra* n. 2, §32.
78 Archick, *supra* n. 18, at 16-17.

 DOI: 10.17103/sybil.19.14

change was merely superficial; it was quantitative rather than qualitative. For instance, in the 2007 agreement, "[t]icketing information, including ticket number, one-way tickets and automated ticket fare quote" constituted one data type, whereas in the 2004 agreement, this comprised four separate data types.[79] As such, the EU was unsuccessful in this battle.

The DPD prohibits processing sensitive data, that is, personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" and provides for some exceptions to this rule.[80]Under the 2004 agreement, the DHS could not use sensitive data collected under the PNR agreement. In the 2007 and 2011 agreements, the US authorities could access sensitive data on, for example, a passenger's racial or ethnic origin, or political or religious affiliations, in specific situations.[81]Under the 2011 PNR agreement, sensitive data used for a specific investigation, prosecution or enforcement action may be retained for however long US law specifies.[82] If not used for one of these specific purposes, sensitive data must be deleted within 30 days of collection.[83] Whilst US authorities maintain that they regularly filter sensitive data out of their computer systems, they acknowledge such data might be useful if the authorities are alerted to "passengers who request wheelchairs hiding bombs in leg casts, or a warning about a threat to a political gathering, or a health emergency affecting people with communicable diseases such as tuberculosis".[84] The DPD does permit the processing for sensitive data for medical purposes, but this is completely unrelated to the aim of the PNR agreement, so it could possibly threaten the necessity principle.[85]

(5) Data Transmission

In something of a rare victory, the EU was successful in changing the data transmission method to protect its data protection values, although only to a certain extent. The 2004 PNR agreement introduced the "pull" method of obtaining PNR data, whereby the US DHS would retrieve the relevant information from airlines. The 2007 PNR agreement, however, obliged airlines to supply US authorities with the relevant information. The former "pull" method was subject to strong criticism from the EU, so EU officials welcome the latter "push" method.[86] Unlike the 2007 agreement, however, which stipulates that the DHS will immediately adopt the "push" system, the 2011 agreement includes a clause stipulating "where necessary, on a case-by-case basis" the DHS may require access to data, which recalls the initial "pull" method, albeit on a far more restricted basis.[87]

---

79 Hornung and Boehm, *supra* n. 8, at 14.

80 DPD, *supra* 6, Art. 8(1).

81 Archick, *supra* n. 18, at 16-17.

82 2011 PNR agreement, *supra* n. 1, Art. 6(4).

83 *Ibid*., Art. 6(4).

84 P. Lewis and S. Hsu, 'Travelers Face Greater Use of Personal Data', *Washington Post*, 27 July 2007 *text available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/07/27/AR2007072700159.html.

85 DPD, *supra* n. 6, Art. 8(3).

86 Archick, *supra* n. 18, at 16-17.

87 Cf.2007 PNR agreement, Art. 2 and 2011 PNR agreement, Art. 15(5).

(6) Judicial Redress

Under the 2011 PNR accord, any data subject whose data has been processed in a way that violates the accord is entitled to effective administrative and judicial redress under US law.[88] During negotiations, EU officials took issue with redress opportunities for EU citizens whose data was processed in the US. The 2011 PNR agreement does not create any right or benefit under US law for any public or private person or entity.[89] As such, EU officials have questioned whether adequate and effective redress policies exist under US law. Furthermore, as the US Privacy Act does not apply to EU citizens, it is questionable whether other US statutes would provide a sufficiently high level of data protection to EU citizens' data.[90] That said, the 2007 agreement outlines a DHS policy choice to "to extend administrative Privacy Act protections to PNR data stored in the ATS", without prejudice to a data subject's nationality.[91] Whilst the 2011 agreement does not explicitly refer to the US Privacy Act, it mentions various related US Acts and "other applicable provisions of US law", thereby potentially including the US Privacy Act.[92]EU pro-privacy commentators have argued that "the practical enforcement of remedies in the US for EU citizens is difficult", thereby questioning how effective US redress opportunities would be in practice.[93] Nonetheless, and not unexpectedly, US officials asserted the May 2011 draft accord provided enhanced legal certainty for passengers seeking redress.[94] Meanwhile, the EU has continued to push for improved redress opportunities for its citizens, especially in reaction to the 2013 Snowden revelations.[95]

CONCLUSION

Whilst the PNR agreements reflect many original US demands, the EU's continual renegotiation efforts show it remains dissatisfied with the agreements' lack of data protection. Seeing as the CJEU annulled the DRD and invalidated the Safe Harbour agreement, and the European Parliament referred the Canada-EU PNR agreement to the CJEU to assess its adherence to EU treaties and the EU Charter, it is increasingly apparent that the 2011 US-EU PNR agreement does not uphold EU data protection principles. It appears the political will to address this shortcoming is growing in the EU. The foregoing shows how the agreement could be modified to better adhere to these principles and ultimately to better protect EU citizens. The PNR agreement negotiations have been a constant struggle between US-EU values and laws. If the EU could ensure its data protection principles are affirmed in any subsequent PNR data sharing arrangement, this would appear to be an extraterritorial diffusion of its law. This diffusion, however, is necessary to protect EU citizens' fundamental right to

88 2011 PNR agreement, *supra* n. 1, Art. 13.
89 *Ibid.*, Art. 21(1).
90 Hornung and Boehm, *supra* n. 8, at 7.
91 2007 PNR agreement, *supra* n. 4, letter from US to EU, Art. IV.
92 2011 PNR agreement, *supra* n. 1, Art. 2(3).
93 Boehm and Cole, *supra* n. 32, at 65.
94 Archick, *supra* n. 18, at 18.
95 See, e.g., M. Gidda, 'Edward Snowden and the NSA files – timeline', *The Guardian*, 21 August 2013.

 DOI: 10.17103/sybil.19.14

data protection, especially when their personal data is processed on US soil, where this right could be threatened.

 DOI: 10.17103/sybil.19.14