EU Exclusive Jurisdiction on Surveillance related to Terrorism and Serious Transnational Crime, Case Review on Opinion 1/15 of the CJEU

Elspeth Guild*

Elif Mendos Kuşkonmaz*

Abstract

This case review examines the Opinion by the Court of Justice of the European Union (CJEU) published on 26 July 2017 on the legal basis of an international agreement signed between the EU and Canada providing for the transfer of information on passengers taking flights from the EU to Canada and the compatibility of that Agreement with the EU fundamental rights, particularly the rights to respect for private life and to protect personal data. Rather spectacularly, the CJEU struck down the Agreement, finding the legal basis inadequate and the terms incompatible with the EU privacy and data protection guarantees. This case review starts by providing a backdrop for the conclusion of the PNR Agreement concerned and for the CJEU's Opinion on that Agreement. Then it moves on to analysing the procedural and substantive aspects of the Opinion and finishes with an analysis of the consequences regarding counter-terrorism measures and for the future of the exchange of personal data in the field of fight against terrorism and serious transnational crime. It is argued here that although Opinion 1/15 deviated from the standard of judicial review established by the CJEU in *Digital Rights Ireland*, *Schrems*, and *Tele2*, it should be considered as a step towards protecting the EU fundamental rights due to the tight procedural conditions for the legality of data sharing agreements it introduced and the high risk of litigation following it.

* Jean Monnet Professor ad personam at Queen Mary, University of London and at the Radboud University Nijmegen. Professor Guild is also Associate Senior Research Fellow at Center for European Policy Studies.

* PhD Student at Queen Mary, University of London.

I Introduction

Since the attacks in the USA on 11 September 2001, states' interest in information on individuals crossing the borders has grown exponentially. This interest has amplified concerns regarding the legitimacy of the interference with the private lives of individuals, yet more often than not, states have invoked national security as a justification permitting them to take measures of questionable compatibility with the right to privacy as part of their border controls. Using Passenger Name Records (PNR) data, which is an umbrella term to cover a wide array of information about air passengers far beyond the mere identity including but not limited to reservations and travel information, has been at the forefront of these concerns. The quest for the PNR data started in the USA and then spread to other states, within and outside the EU.[1] The agreement negotiated between the EU and Canada on the transfer and use of those data was a result of this spread. Its challenge before the Court of Justice of the European Union (CJEU) has unravelled a range of issues. The key issues are the CJEU's emphasis on the law enforcement aspect of counter-terrorism action, a possible carve out the concept of "terrorism" from the general field of national security and its place near EU police co-operation. Secondly, in the Opinion that is the subject of this article, the CJEU set out a list of procedural requirements which any agreement covering the transfer of personal data to a non-EU Member State for the purpose of the fight against terrorism and serious transnational crime must meet in order to comply with the EU fundamental rights of privacy and personal data protection.

[1] The United Kingdom, Sweden, and Belgium are the EU Member States with a fully functioning national PNR scheme. European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime' COM(2011) 32 final.

This case review examines the CJEU's Opinion on the conclusion of the Canada PNR Agreement.[2] In this context, it provides a background to the Opinion, followed by its summary and commentary.

II Background to the Opinion

As a response to and in solidarity with the USA following the attacks in New York and Washington D.C. on 11 September 2001, Canada enacted a law that obliged air carriers to transfer the information on Canada-bound air travel passengers to the Canadian border control authority, Canada Border Service Agency (CBSA).[3] This information is called the Passenger Name Record (PNR) and it is generated by passengers, their travel agencies, and their air carriers when those passengers book, check-in, and board a flight.[4] PNR includes a wide array of information ranging from passengers' names, their addresses, the means of payment for the flight, or any travel-related preferences made by passengers as in-flight meal choices or wheel-chair requests.[5]

The Canadian law obliging the transfer of the PNR data was potentially at odds with the EU rules on data transfers to third countries, which are permitted only insofar as that third country has an adequate level of protection for personal data as guaranteed in the EU.[6] The European Commission was conferred the power to determine whether the third country

---

[2] Opinion 1/15 of the Court (Grand Chamber) ECLI:EU:C:2017:592 [2017].

[3] See, the Anti-Terrorism Act 2001. For information on the issue see; Peter Hobbing, 'Tracing Terrorists: The EU-Canada Agreement in PNR Matters', (CEPS, September 2008) <http://aei.pitt.edu/11745/1/1704.pdf> (accessed 29 November 2017).

[4] International Civil Aviation Organization, 'Guidelines on Passenger Name Record (PNR) Data' (2010) available at <https://www.iata.org/iata/passenger-data-toolkit/assets/doc_library/04-pnr/New%20Doc%209944%201st%20Edition%20PNR.pdf> (accessed 29 November 2017).

[5] *ibid.*

[6] Art. 25 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23 November 1995 [hereinafter, 'Data Protection Directive'].

guaranteed the required level of protection.[7] However, the European Commission had not exercised it for Canada. Therefore, without an adequacy finding by the European Commission, the air carriers were in breach of EU law if they transferred the PNR data to Canada. They were also in breach of the Canadian law requiring them to disclose the PNR data to the CBSA.

To settle the dispute, the European Commission and the CBSA started to negotiate an agreement with the aim of ensuring that PNR data could be transferred to the CBSA, whilst the fundamental rights of the individuals were protected in accordance with the EU standards. The results of these negotiations were a time limited adequacy decision[8] adopted on 6 September 2006 by the European Commission in accordance with the powers conferred to it under the Data Protection Directive 95/46[9] (will be replaced by the General Data Protection Regulation in May 2018[10]), and the international agreement, which entered into force in March 2006.[11]

This Agreement allowed for the transfer of PNR data of all passengers flying from the EU to Canada, the subsequent retention and use of such data for the purpose of countering terrorism and serious transnational crime.[12] Once the PNR data were acquired by the CBSA,

[7] Article 25 (5) and (6) of the Data Protection Directive (n 6).

[8] Commission Decision 2006/253/EC 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] OJ L91/49 [hereinafter, 'Decision 2006/253'].

[9] Data Protection Directive (n 6).

[10] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[11] Council Decision 2006/230/EC of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data [2006] OJ L82/14; Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data [2006] OJ L 82/15 [hereinafter, '2006 Canada PNR Agreement'].

[12] Arts 1, 3, and 5 of the 2006 Canada PNR Agreement (n 11).

they were processed to identify passengers who posed a risk to public security, but who were not known by the CBSA.[13]

The adequacy decision, and consequently the 2006 Agreement, expired in 2009[14], but the CBSA agreed to abide by the data protection commitments underpinning the adequacy decision until the conclusion of a new agreement.[15] The negotiations for a new agreement started following a European Commission's Communication of 21 September 2010[16] and the European Parliament's resolution of 11 November 2010.[17] After four years of negotiations, the new agreement between the EU and Canada on the transfer of PNR data was signed on 25 June 2014.[18] In order for this Agreement to be effective for the EU, the European Parliament had to approve it. However, the changed political landscape on international personal data transfer after the revelations of mass surveillance by USA intelligence authorities made by Edward Snowden in 2013 was nowhere more evident than in the European Parliament.[19] Therefore, instead of approving it, the European Parliament adopted a resolution on 25 November 2014 seeking an opinion from the Court of Justice of the European Union on

[13] Hobbing (n 3) 15-17.

[14] Art. 7 of the Decision 2006/253 (n 8) ("This Decision shall expire three years and six months after the date of its notification, unless extended in accordance with the procedure set out in Article 31(2) of Directive [95/46], Agreement 5(1) and 2.")

[15] Arianna Vedaschi and Gabriele Marino Noberasco, 'From DRD to PNR: Looking for a New Balance Between Privacy and Security' 67-90, in: David Cole, Federico Fabbrini, and Stephen Schulhofer (eds), *Surveillance, Privacy and Trans-Atlantic Relations*, (Hart Publishing, 2017).

[16] European Commission, 'Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries', COM(2010) 492.

[17] European Parliament Resolution of 11 November 2010 on the global approach to transfers of passenger name record (PNR) data to third countries, P7_TA(2010)0397.

[18] For the difference between the agreements signed with Canada in 2006 and in 2014 see; Vedaschi and Noberasco (n 15).

[19] For the European Parliament's response to those revelations 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', P7_TA(2014)0230, (21 February 2014).

whether the draft Agreement was compatible with EU fundamental rights and whether it had been concluded on an appropriate legal basis.[20]

III The Opinion of the CJEU

The transfer of personal data outside the EU has been in the spotlight since the CJEU's *Schrems* decision, which struck down in 2015 the European Commission's adequacy finding on the basis of which the Safe Harbour principles for the personal data transfers from the EU to US businesses had been considered as compliant with the EU standards.[21] On 26 July 2017, the CJEU added another brick to the privacy wall concerning the personal data transfers to a non-EU Member State country in its Opinion on the draft agreement between the EU and Canada on the transfer of PNR data, their subsequent access and use for the purpose for countering terrorism and serious transnational crimes. This section reviews this Opinion and consists of two sub-section (a) the procedural part and (b) substantive part of the Opinion.

A The Procedural Part of the Judgment: The Question on the Appropriate Legal Basis

In its lengthy and rather technical assessment of the appropriate legal basis for the conclusion of the Canada PNR Agreement, the CJEU dealt with issues that may have far-reaching impacts in the field of EU counter-terrorism, and on the legality of the existing PNR agreements with other countries. The CJEU put emphasis on the relation between the transfer and use of information in the context of combatting terrorism and serious transnational crime and police co-operation in criminal matters when determining the correct legal basis for the

[20] European Parliament, 'MEPs refer EU-Canada air passenger data to the EU Court of Justice', (25 November 2014) Press Release available at <http://www.europarl.europa.eu/news/en/press-room/20141121IPR79818/meps-refer-eu-canada-air-passenger-data-deal-to-the-eu-court-of-justice> (accessed 29 November 2017).

[21] C-362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [2015]. For commentary see; Tuomas Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter', (2016) 12(2) *European Constitutional Law Review* 318.

Canada PNR Agreement. To make this matter comprehensible, a brief account of the EU counter-terrorism framework is given below.[22] However, it is worth noting here that this emphasis can be considered as the CJEU's willingness to highlight that counter-terrorism action is about not only the security and defence dialogue, but also police co-operation in relation to the prevention, detection, and investigation of criminal offences. Seen from this angle, the CJEU might be ready to consider that insofar as surveillance measures in the field of national security relate to the fight against terrorism and serious transnational crime, authorities must ensure that those measures respect the EU rules on privacy and protection of personal data.

At the outset, the CJEU identified two objectives for the Canada PNR Agreement: ensuring public security by preventing, combatting, repressing, and eliminating terrorism and serious transnational crime, and respecting the fundamental rights of the right to respect for private life and to the protection of personal data.[23] It further observed that the transfer of PNR data to Canadian competent authorities and their subsequent use by those authorities were justified only by the objective of ensuring public security in Canada and in the EU.[24] Moreover, that transfer can only be permissible if the receiving third country such as Canada ensured a level of fundamental rights protection that is essentially equivalent that of afforded in the EU.[25] Based on these observations, the Court held that both objectives that the Agreement pursued were inextricably linked with each other.[26] This means that measures relating to the use of personal data for purposes of fighting terrorism and serious transnational crime have to abide by EU fundamental rights of privacy and protection of personal data obligations.

[22] See section (IV).

[23] Opinion 1/15 (n 2), paras 80-90.

[24] *ibid*., para. 91.

[25] *ibid*., para. 93.

[26] *ibid*., para. 94.

In relation to the objective of respecting fundamental rights (a) to respect for private life and (b) to the protection of personal data, it is no surprise that the CJEU found Article 16 of the Treaty on the Functioning of the European Union (TFEU) as one of the appropriate legal base to conclude the Canada PNR Agreement because that Article covers the right to protection of personal data.[27] The point in placing counter-terrorism within the sphere of police co-operation emerged when the Court held that Article 87(2)(a) of TFEU (police co-operation in criminal matters) was the correct legal base to accommodate the Agreement's objective of ensuring public security. The Agreement provided rules on the transfer and use of data for purposes of prevention, investigation, and detection of terrorism and serious transnational crimes, - a type of information and of data processing that fell within the sphere of Article 87(2)(a) of TFEU.[28]

Thus, the CJEU held that the correct legal basis were Articles 16 and 87(2)(a) of the TFEU, but not Article 82(1)(d) of TFEU on the judicial co-operation in criminal matters (which the European Commission had proposed). Therefore, the Canada PNR was based on an incorrect legal basis. Evidently, this finding casts doubt on the legal basis of the existing data transfer agreements in the field of fight against terrorism and serious transnational crime that refer to the latter article such as agreements signed with the USA[29] and Australia[30] on the transfer of PNR data.[31]

---

[27] Opinion 1/15 (n 2), para. 97.

[28] *ibid*., para. 100.

[29] Agreement between the United States of America and the European Union on the use and transfer of passenger name record to the United States of Department of Homeland Security [2012] OJ L 215/5.

[30] Agreement between the European Union and Australia on the use and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service [2012] OJ L 186/4.

[31] In his opinion on the Canada PNR Agreement, the Advocate General Mengozzi mentioned this issue and noted that the finding relating to Article 82(1)(d) of the TFEU as the incorrect legal basis for concluding the relevant agreement did not mean that PNR data agreement with the USA and Australia that based on the same article were void. He added that 'the legal basis used for the adoption of other Union measures that might

B The Substantive Part of the Judgment: Determining the Compatibility of the EU-Canada PNR Agreement with EU Fundamental Rights

The first time the CJEU was asked about the compatibility of the PNR transfer scheme with privacy and personal data protection rights was in 2006, when the European Parliament challenged the then valid PNR data transfer agreement with the USA.[32] The European Parliament argued that the legal basis for that Agreement was incorrect and that it was in breach of fundamental rights.[33] At the time of the challenge, the Lisbon Treaty had yet to be negotiated, and thus there was no Article 16 of the TFEU or its equivalent. As a result, the Court only addressed the legal basis question, without going further into the complaint in relation to a possible fundamental rights violation.[34]

By 2017, the compliance of the PNR data transfer scheme with fundamental rights post-Lisbon was central for the CJEU in its Opinion 1/15. In the Court's view, the Canada PNR Agreement could not be concluded in its current form because it was incompatible with the EU rights to respect for private life and to protection of personal data. It further provided a list of procedural requirements which any data transfer for the purpose of the fight against terrorism and serious transnational crime must satisfy. The reasoning for these requirements is of great importance for the current and prospective data transfers in the context of fight

---

display similar characteristics is irrelevant.' Opinion of Advocate General Mengozzi in Opinion 1/15 ECLI:EU:C:2016:656 [2016], para. 109.

[32] 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 [2004] OJ L 142 M.

[33] 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 E.C.R I-4721.

[34] It is sufficient to note here that the CJEU could address the complaint on the breach of fundamental rights by referring to Article 8 of the European Court of Human Rights in light of Article 6 (1) of the Treaty on European Union (TEU). See; Cian Murphy, *The EU Counter-Terrorism Law: Pre-Emption and the Rule of Law* (Hart Publishing, 2015) 165-166; Elspeth Guild and Evelien Brouwer, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US', (CEPS No. 109 July 2006) 4-5.

against terrorism and serious transnational crime in general, and the future negotiations for all PNR agreements in particular.

First, the CJEU turned its attention to the impact that the use of PNR data has on the private lives' of individuals concerned. According to the Court, the Canada PNR Agreement permitted '*the systematic and continuous* transfer of PNR data of all passengers flying between the European Union and Canada.'[35] Also, such data as a whole may 'reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide *sensitive information* about those passengers.'[36]

The Court further accepted that PNR data were chiefly used as an intelligence tool.[37] Here, it mentioned two techniques for using those data. The first technique was the systematic and automatic analysis of the transferred PNR data based on the pre-established models and criteria before the flights reach to Canada.[38] The second technique was the crosschecking of those data with other databases, which in turn could reveal additional information on the private lives of the passengers.[39] These techniques were used to identify passengers who may pose a risk to public security, and thus who may be subjected to additional checks at borders.[40] Additionally, the Court stressed that the five-year retention period for the PNR data required under the Canada PNR Agreement constituted a lengthy time for which the information on the private lives of individuals was available.[41]

[35] Opinion 1/15 (n 2), para. 127. [Emphasis added]

[36] *ibid.*, para. 128. [Emphasis added]

[37] *ibid.*, para. 130.

[38] *ibid.*, para. 131.

[39] *ibid*.

[40] *ibid*., para. 132.

[41] *ibid.*

Having observed the aggravated interference resulting from the Canada PNR Agreement with the right to privacy and protection of personal data, the CJEU proceeded to analyse the justification for such interference. At the outset, it clarified the general rules for that justification in light of its settled case-law. Therefore, it referred to Article 8(2) of the Charter of the Fundamental Rights of the European Union (Charter), according to which personal data must be processed 'for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'[42], and to Article 52(1) of the Charter, according to which any limitation on the rights enshrined in it 'must be provided for by law and respect the essence of those rights.'[43] The latter article further required that, subject to the principle of proportionality, such limitation must be necessary and genuinely meet objectives of general interest recognised by the EU.[44] Using its decisions on *Digital Rights Ireland*[45], *Schrems*[46], and *Tele2*[47] as the legal authorities, the CJEU held that the proportionality principle required the limitation on the protection of personal data to apply only insofar as it was strictly necessary. [48] In order to be meet this strict necessity requirement, the contested legislation 'must lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards' against the risk of

[42] Opinion 1/15 (n 2), para. 137.

[43] *ibid*., para. 138.

[44] *ibid*.

[45] Joined Cases C293/12 and C594/12 *Digital Rights Ireland v. The Minister for Communications, Marine and Natural Resources and Others* ECLI:EU:C:2014:238 [2014]. For commentary see; Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection' (2014) 39(6) European Law Review 835.

[46] Schrems (n 21).

[47] C-203/15 *Tele2 Sverige AB v. Post –och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others* ECLI:EU:C:2016:970 [2016]. For commentary see; Iain Cameron, 'A Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson', (2017) 54(5) *Common Market Law Review* 1467.

[48] Opinion 1/15 (n 2), para. 140.

abuse, and must elaborate 'in what circumstances and under which conditions a measure providing for the processing of such data may be adopted.'[49]

Having considered the general principles on the limitation on the rights to respect for private life and to protection of personal data, the CJEU went on to consider the details of the Canada PNR Agreement. When determining the legal basis upon which the PNR data were processed, the Court rejected the argument that the passengers' consent qualified as a basis as such because that consent was given in relation to the collection of their data for reservation purposes and not for the transfer of those data to Canada.[50] The Agreement did not provide for the PNR data transfer on the condition of passengers' consent, and therefore that transfer had to be based on some other legal basis within the meaning of Article 8(2) of the Charter.[51] According to the Court, the Canada PNR Agreement constituted that basis.[52] It is worth noting here that even if the Agreement had required such consent requirement, the CJEU might have made the same conclusion because the validity of the consent obtained by air carrier companies in the online environment would have come under scrutiny. The crux of the validity question is that individuals are not able to reserve flights unless certain information is disclosed and used for purposes other than they have expected. Therefore, their consents for the processing of that information (i.e. PNR data) are invalid as they were not given freely and fully informed.[53]

---

[49] Opinion 1/15 (n 2), para. 141.

[50] *ibid*., paras 142-143.

[51] *ibid*., para. 144

[52] *ibid*., para. 147.

[53] Under EU data protection laws, consent must be freely given, informed, and explicit. Article 29 Working Party, which is the EU's data protection authority, dealt with the passengers' consent during the negotiations for the PNR agreement with the USA in 2002 and held that such consent was invalid because passengers had no choice of agreeing with the processing of PNR data if they wishes to fly to the USA, and thus their consent was not given freely. See; Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent', 01197/11/EN WP187, (13 July 2011) available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf> (accessed 29 November 2017), 16.

The next stage on the compatibility question was the existence of an objective of general interest carried out by the Canada PNR Agreement. At this point, the CJEU reiterated its earlier statement and noted that the transfer and use of those data under the Agreement were carried out in order to ensure public security, which was an objective of general interest that is capable of justifying even serious interferences with Articles 7 and 8 of the Charter.[54] Moreover, it accepted that the transfer and use of PNR data under the Agreement were appropriate for enhancing public security as those data facilitated security and border control checks. [55] In its earlier paragraphs, the Court referred to the information provided by the CBSA on the number of arrests made for almost a year. Accordingly, between April 2014 and March 2015, 28 million air passengers travelled from the EU to Canada and out of those passengers 178 arrests were made, 71 drug and 2 child pornography material seizures were carried out, and for 169 further investigations in relation to terrorism were made.[56]

The acceptance by the CJEU of the appropriateness of the PNR data transfer scheme is interesting because the information given above suggests that there is a disproportion between the vast number of passengers travelling to Canada and the low number of cases in which the PNR data proved of any use in the fight against terrorism and serious transnational crime. This is of great importance when determining the proportionality of the interference caused by the Canada PNR Agreement, but the CJEU did not consider this issue. Perhaps it is keeping its power dry for another case. Another issue is that the appropriateness of the PNR data transfer scheme is contestable, despite what the CJEU held in Opinion 1/15. The European Data Protection Supervisor (EDPS)'s observation on the Canada PNR Agreement

[54] Opinion 1/15 (n 2), para. 149.

[55] *ibid*., paras 152-153.

[56] *ibid*., para. 54.

is instructive in this regard.[57] In this context, the EDPS noted that '[he] has not seen convincing elements showing the necessity and proportionality of the massive and routine processing of data of non-suspicious passengers for law enforcement purposes.'[58] In tune with the EDPS, the Article 29 Working Party observed the absence of objective statistics proving the use of PNR data in the fight against terrorism and serious transnational crime when addressing the transfer of those to third countries from a data protection point of view.[59] Interestingly, the CJEU also mentioned in the Opinion at hand that the European Commission and the Council did not have precise statistics showing that the use of PNR data contributes to the fight against terrorism and serious transnational crime.[60] Therefore, it is hard to reconcile the CJEU's final observation on the appropriateness of the PNR data transfer scheme.

Moving on to the next stage on the compatibility question on determining whether the interference cause by the contested measure was proportionate to achieve the aim that measure pursued, the CJEU laid down the limitations for the transfer and use of PNR data in light of the strict necessity test. In this regard, it observed that the categories of PNR data to be transferred under the Canada PNR Agreement had to be defined clearly and precisely. The Agreement did not meet this requirement because some categories such as 'available frequent flyer and benefit information (free tickets, upgrades, etc.)', 'all available contact information (including originator information)' and 'general remarks including Other Supplementary

[57] Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record Data, (EDPS, 30 September 2013) available at <https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf> (accessed 29 November 2017).

[58] *ibid*., note 3.

[59] Article 29 Data Protection Working Party, 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries', 622/10/EN WP178 (12 November 2010), 3 available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf> (accessed 29 November 2017).

[60] Opinion 1/15 (n 2), para. 55.

Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information' failed to delineate the scope of transferred data.[61] As regards the sensitive data, which cover the information relating to 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or concerning a person's health or sex life[62], the CJEU noted that the Canada PNR Agreement did not directly involved the data of this nature.[63] Nevertheless, the fact remained that the Agreement could provide for the transfer of such data because the OSI, SII, and SSR information could include information on passengers' in-flight meal choices (i.e. halal or kosher food) or wheelchair assistance, which in turn was capable of revealing information on religious beliefs or person's health.[64] For this reason, the CJEU argued that the Agreement carried the risk of infringing the principle of non-discrimination as enshrined in Article 21 of the Charter.[65] This meant that the transfer of sensitive data under the Agreement had to be based on 'a precise and particularly solid justification', rather than merely referring to the protection of public security against terrorism and serious transnational crime.[66] The Agreement lacked such justification, and thus the transfer of sensitive data to Canada, their use and retention by the Canadian authorities under it were incompatible with the Charter.[67]

At the next stage of the proportionality assessment, the CJEU noted some points on the pre-established models upon which such processing is made, the results achieved by those

[61] Opinion 1/15 (n 2), paras 156-163.

[62] Art. 8 of the Canada PNR Agreement.

[63] Opinion 1/15 (n 2), para. 164

[64] *ibid.* See also; Opinion of the European Data Protection Supervisor 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 of Homeland Security, (EDPS, 9 December 2011) available at <https://edps.europa.eu/sites/edp/files/publication/11-12-09_us_pnr_en.pdf> (accessed 29 November 2017), note 11.

[65] Opinion 1/15 (n 2), para. 165.

[66] *ibid*.

[67] *ibid*., para. 167.

models, and the databases utilised for crosschecking. First of all, it held that the pre-established models should be specific and reliable.[68] Secondly, the results made in light of them must identify individuals on the basis of a reasonable suspicion of participation in terrorist offences and transnational crimes, and these results must be compatible with the principle of non-discrimination.[69] Thirdly, the databases utilised for crosschecking the PNR data 'must be reliable, up to date, and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime.'[70] Fourthly, given that the data analysis made on the basis of the automated processing of PNR data involved some margin of error, any positive result must be re-examined by an individual before a measure adversely affecting a passenger is made.[71] Lastly, in the view of the CJEU, all the mentioned points should be included in the joint review of the Canada PNR Agreement.[72]

Regarding the purposes for which the PNR data are processed, the CJEU was of the opinion that the definitions of terrorist offences and serious transnational crimes were sufficiently clear and precise.[73] However, the Canada PNR Agreement contained other purposes for which the PNR data may be processed. The processing for the protection of the vital interests of any individual including a significant public health risk was one of those purposes and the Court held that this purpose was defined sufficiently clear, despite the fact that it also covered interests other than countering terrorism and serious transnational crime.[74] That said, it further stated that the processing of the PNR data on a case-by-case basis to 'ensure the oversight or accountability of the public administration' and to 'comply with the

[68] Opinion 1/15 (n 2), para. 172.

[69] *ibid.*

[70] *ibid.*

[71] *ibid*., para. 172.

[72] *ibid.*

[73] *ibid.*, paras 177-178.

[74] *ibid.*, para. 180.

subpoena or warrant issues, or an order made, by a court' was 'too vague and general to meet the requirements as to clarity and precision required.'[75] Another issue relating to the scope of the rules for processing of PNR data was the identities of the competent Canadian authorities for such processing, which the Court found as sufficiently and clearly defined.[76]

The CJEU then went on to analyse the extent of the transfer of PNR data of all air passengers flying from the EU to Canada. It is important to note here that in its *Schrems* and *Tele2* decisions, the CJEU acknowledged that EU law precluded the generalised and indiscriminate retention of personal data and access to those data by public authorities.[77] In this regard, such retention and access must be limited based on a connection between those data and the participation of persons concerned with terrorism and serious crimes.[78] In relation to the transfer of PNR data of all air passengers, the Court accepted that this untargeted transfer was EU fundamental rights complaint. The reason for this finding boiled down the principal aim of the automated PNR data analysis, which was to identify who are unknown to Canadian authorities, and who pose a potential public security risk, and thus may be subject to further examination at the border.[79] In view of the Court, excluding certain passengers or certain areas of origin would be detrimental in achieving this aim.[80] For this reason, the transfer of PNR data of all passengers, regardless of their criminal background was permissible.

---

[75] Opinion 1/15 (n 2), para. 181.

[76] *ibid*., paras 182-185.

[77] For a brief review on the EU standards for data retention measures for law enforcement purposes in light of EU fundamental rights of privacy and data protection see; Franziska Boehm, 'Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes', (2016) 2(2) *European Data Protection Law Review* 178.

[78] Schrems (n 21), para. 93; Tele2 (n 47), paras 105, 111, and 118.

[79] Opinion 1/15 (n 2), para. 187.

[80] *ibid.*

By contrast, the CJEU did not accept the retention and use of PNR data of all passengers once they had been admitted to Canada. It limited the use of those data to the time when the passenger concerned is in Canada and to the 'new circumstances justifying that use.'[81] There must be substantive and procedural conditions and circumstances based on objective criteria under which the Canadian authorities can perform further use of PNR data as such.[82] Further, a court or an administrative authority must approve the access to those retained data on the basis of a reasoned request made by those authorities.[83] That reason must be limited to the prevention, detection, or prosecution of crime.[84]

In relation to the retention and use of PNR data after passengers' departure from Canada, the CJEU noted that the required connection between the personal data and the objective pursued did not exist because passengers had already been verified as a non-security risk in light of their PNR data upon their arrival to and during their stay in Canada.[85] For this reason, in principle, the continued retention of PNR data of passengers on their departure from Canada was unjustified unless passengers present a risk as regards terrorism and serious transnational crime on the basis of objective evidence.[86] That further access must be subject to substantive and procedural conditions based on objective criteria under which the Canadian authorities can have access to those data stored beyond passengers' stay in Canada.[87] A court or an independent administrative body must grant such access.[88] With regards to the length of time for which the PNR data are retained, the CJEU held that the five-year retention was justified because the lifespan of investigating serious crime networks

[81] Opinion 1/15 (n 2), para. 200.

[82] *ibid.*

[83] *ibid*., para. 202.

[84] *ibid.*

[85] *ibid*., paras 204-205.

[86] *ibid*., paras 205-207.

[87] *ibid*., para. 208.

[88] *ibid*.

could be lengthy and complex.[89] Moreover, the continued retention of PNR data after passengers concerned have left Canada was justified on the condition that those data were kept in Canada and were irreversibly destroyed at the end of the retention period.[90]

Regarding the disclosure of the PNR data to government authorities of other third countries, the CJEU reiterated its finding in *Schrems*[91] that the data transfers to a third country is permissible if that country affords an essentially equivalent data protection to that guaranteed in the EU.[92] Following this, the CJEU considered that this required level of protection applied to PNR data transfers from Canada to third countries.[93] From thereon, it found that the Canada PNR Agreement did not meet the strict necessity requirements because it conferred a discretionary power to the competent Canadian authority to assess the level of data protection afforded in third countries even if a positive finding by the EU on that level does not exit, which in turn carried the risk of circumventing the 'essentially equivalent protection' requirement.[94] The disclosure of PNR data to the third persons was also not strictly necessary because the conditions for such disclosure were defined vaguely.[95]

The CJEU further considered passengers' rights to access their PNR data and to have them rectified. It noted that these rights were linked with the rights of those passengers to be informed of the transfer and the use of their PNR data once the risk of jeopardising the investigation disappears.[96] It observed that although the Canada PNR Agreement contained provisions on the right to access and correction, it did provide a notification procedure for individuals. According to the CJEU, the transparency provision under the Canada PNR

[89] Opinion 1/15 (n 2), para. 208.

[90] *ibid*., para. 210.

[91] Schrems (n 21).

[92] Opinion 1/15 (n 2), para. 214.

[93] *ibid*.

[94] *ibid*., paras 212-214.

[95] *ibid*., paras 216-217.

[96] *ibid*., paras 218-220.

Agreement was insufficient in satisfying such procedure for the passengers, because it merely referred to the transfer and use of PNR data for the purposes of security checks and border controls. In this context, the passengers were not notified of the situations in which the PNR data are used for the purposes beyond those checks and controls.[97] Furthermore, the CJEU was satisfied with the remedies that the Canada PNR Agreement provided for the passengers.[98] However, it observed that the Agreement failed to provide in a sufficiently clear and precise manner that the oversight mechanism carry out its task independently as enshrined in Article 8(3) of the Charter.[99]

Overall, the procedural requirements that the Court seeks in the Canada PNR Agreement in particular and in data transfer schemes for the fight against terrorism and serious transnational crime are the following[100]:

- The categories of PNR data to be transferred must be defined clearly and precisely.
- The pre-established models through which the PNR data are automatically analysed must be specific, reliable, and non-discriminatory.
- The use of PNR data is limited to the fight against terrorism and serious transnational crime.
- There must be substantive and procedural conditions based on objective criteria against which the PNR data can be used and accessed by public authorities after

[97] Opinion 1/15 (n 2), paras 222-223.

[98] *ibid*., paras 226-227.

[99] *ibid*., paras 228-231. On the importance of an independent oversight mechanism for the protection of personal data and how that mechanism qualifies as such see; Marek Szydlo, 'The independence of data protection authorities in EU law: between the safeguarding of fundamental rights and ensuring the integrity of the internal market' (2017) 42(3) *European Law Review* 369.

[100] Opinion 1/15 (n 2), para. 232.

the passenger concerned is admitted to the country. Court or independent administrative body must review that use and access a priori.

- The continued retention of PNR data is permitted only if there is objective evidence that the passenger concerned present a risk on the grounds of terrorism and serious transnational crime.
- The PNR data can only be disclosed to a competent authority in a non-EU country if it has an agreement with the EU equivalent to the Canada PNR Agreement, or it benefits from a positive adequacy finding by the European Commission.
- It must be ensured that the passengers are notified individually of the use of their PNR data.
- There must be independent oversight mechanisms over the implementation of the Canada PNR Agreement.

IV Commentary

The implications of the CJEU's opinion on the Canada PNR Agreement is wide-ranging. One certain implication is that the European Commission will have to re-negotiate the Agreement in light of the criteria under which the transfer of personal data for the purpose of fight against terrorism and serious transnational crime is considered as legal in EU law.[101] The European Parliament's attitude in the aftermath of Opinion 1/15 is interesting in understanding the direction that the discourse surrounding the Canada PNR Agreement could go. On the one hand, there were strong voices for privacy protection that called on the prevalence of privacy rights in the future renegotiation stage.[102] On the other hand, there were

[101] The Commissioner for Security Union, Julian King, accepted this point. See; European Commission, 'EU-Canada PNR agreement: Commission statement on the Opinion of the European Court of Justice' (26 July 2017), Press Release available at <http://europa.eu/rapid/press-release_STATEMENT-17-2105_en.htm> (accessed 29 November 2017).

[102] The European Parliament Rapporteur on the Canada PNR Agreement, Sophie in't Veld MEP said that '[Opinion 1/15] shows that anti-terror laws are all too often made in haste, but are then unable to pass judicial

those voices emphasising the higher value of security over privacy rights, whilst having welcomed the CJEU's Opinion.[103] How these conflicting views will play out in the European Parliament remains to be seen.

Moreover, the CJEU's findings in relation to the legal basis of the Agreement raises questions on the general mandate of EU in relation to counter-terrorism measures. It is worth noting here that this mandate is scattered across the EU's different competencies.[104] These include police and judicial co-operation in criminal matters and EU's Common Foreign and Security Policy.[105] What this scattered legal framework means is that there is a tension between law enforcement co-operation and defence dialogue at the EU level.[106] As the extent of oversight of the counter-terrorism measures would differ depending on the legal framework under which they are adopted, it is difficult to ascertain that fundamental rights obligations are respected when implementing those measures. This issue brings to the surface particularly at the EU-internal level how terrorism is identified as a threat to the EU Member

---

review. Privacy rules and fighting terrorism do not have to contradict one another, but laws must be made with due observance of European standards and values.' See; European Parliament, 'Rapporteur welcomes court's rejection of EU Canada passenger data deal' (26 September 2017) Press Release available at <http://www.europarl.europa.eu/news/en/press-room/20170726IPR80601/rapporteur-welcomes-court-s-rejection-of-eu-canada-passenger-data-deal> (accessed 29 November 2017).

[103] The EPP Group's Rapporteur for the Canada PNR Agreement, Axel Voss MEP said that 'on the issue of the fight against terrorism, the protection of the data of all citizens is less important than the protection of the individual.' See; EPP Group, 'EU court ruling confirms Canada PNR agreement', (26 September 2017) Press Release available at <http://www.eppgroup.eu/press-release/EU-Court-ruling-confirms-Canada-PNR-agreement> (accessed 29 November 2017).

[104] Murphy (n 34), 21; Javier Argomaniz, *The EU and Counter-Terrorism: Politics, polity, and policies after 9/11*, (Routledge, 2011) 139.

[105] Titles VI and V of the Treaty on the European Union. On the historical evolution of the EU's counter-terrorism policies see; Wim Wensink et al, 'The European Union's Policies on Counter-Terrorism: Relevance, Coherence and Effectiveness', (Study for the LIBE Committee, January 2017) available at <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583124/IPOL_STU(2017)583124_EN.pdf> (accessed 29 November 2017).

[106] J. Monar, 'Common Threat and Common Response? The European Union's Counter-Terrorism Strategy and its Problems' (2007) 42 *Government and Opposition* 292, 294.

States' national security, which is firmly lies within their competence.[107] As a result, there is a strong claim that their actions for the fight against terrorism fall outside the scope of EU law and the jurisdiction of the CJEU. Opinion 1/15, however, may be read as the CJEU's first salvo towards this mantra. As a starting point, the Court highlights the link between the police co-operation in criminal matters and the protection of public security through fighting terrorism and serious transnational crime, which seems to indicate a tilt towards counter-terrorism measures as part of the police co-operation dimension. The CJEU's further move of linking the objective of personal data protection and police co-operation suggests that the Court sees the EU fundamental rights of privacy and personal data protection obligations as the constraints on counter-terrorism measures involving the transfer and use of personal data. Taking the argument a bit further, perhaps it can be suggested that the CJEU is willing to carve out the terrorism threat from the concept of national security interest, and take surveillance measures in relation to that interest within the remit of EU police co-operation when they are carried out for the purpose of the fight against terrorism.[108] Hopefully, the CJEU will have the opportunity to elaborate more on this national security based division of competences in relation to the surveillance measures in the near future. The UK Investigatory Powers Tribunal (IPT), which is the oversight authority for the surveillance practices of the UK public authorities, has already referred a question on this matter to the CJEU.[109] It might

[107] Art. 4 of the TEU.

[108] The question on the applicability of EU law over surveillance measures in the field of national security is an ongoing issue. Article 29 Data Protection Working Party, 'Working Document on surveillance of electronic communications for intelligence and national security purposes', 14/EN WP228 (5 December 2014) available at <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf> (accessed 29 November 2017).

[109] Privacy International v. Secretary of State for Foreign and Commonwealth Affairs et al. [2016] UKIPTrib 15_110-CH; available at <http://www.ipt-uk.com/docs/Privacy%20International%20v%20SSFCA%20and%20Ors%20September%202017.pdf> (accessed 29 November 2017).

take some years before the CJEU gives an answer because the IPT did not expedite this reference and the negotiations of the UK's leave from the EU might take precedence.[110] Nevertheless, when it does answer the question, the CJEU will inevitably have an impact on the future of the surveillance measures in the context of countering terrorism.

Another impact of the Opinion is that it comes as a challenge to the scope of the transfer and use of personal data schemes for purposes of fight against terrorism in general. Existing schemes falling short of the requirements established in this Opinion are incompatible with EU fundamental rights. These schemes include the Terrorist Finance Tracking Program Agreement with the USA on transfer of financial data[111] and agreements signed with the US[112] and Australia[113] on PNR data transfers. Conflicts between these agreements and the CJEU's findings in its Opinion at hand imperils their legality in EU law.[114] The same arguments may also be made with regards to other data transfer schemes such as the Privacy Shield[115] and the Umbrella Agreement[116] as well as to the EU's own

[110] For an analysis on the implications of the UK's leave from the EU over the UK data protection landscape see; Andrew Murray, 'Data transfers between the EU and UK post Brexit?' (2017) 7(3) *International Data Privacy Law* 149.

[111] 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, [2010] OJ L 195/5.

[112] The EU-US PNR Agreement (n 29).

[113] The Australia PNR Agreement (n 30).

[114] A call on suspending the PNR data transfer agreements with the USA and Australia has already been made. EDRi.org, 'PNR: EU Court rules that draft EU/Canada air passenger data deal is unacceptable', (26 July 2017) Press Release available at <https://edri.org/pnr-eu-court-rules-draft-eu-canada-air-passenger-data-deal-is-unacceptable/> (accessed 20 November 2017).

[115] This data transfer scheme replaces the now invalid Safe Harbour principles and provides the legal basis for the transfer of personal data from the EU to the US businesses. Its legality has already been question before the CJEU after *Schrems*. See; T-670/16 *Digital Rights Ireland v Commission*; T-281/16 *La Quadrature du Net and Others v Commission*.

[116] This Agreement provides a data protection framework for the transfer of personal data between the US and the EU competent law enforcement authorities. The EDPS recommended improvements for the Agreement to be EU fundamental rights-compliant. See; Opinion 1/2016 of the European Data Protection Supervisor on

internal PNR scheme.[117] On the same line, any future international agreement on the data transfer has to meet with the criteria set out in Opinion 1/15 to be legal in EU law. For this reason, the Opinion has been referred to as a 'significant victory for the fundamental rights to privacy and data protection.'[118]

Indeed, the Court's consistent reference to *Digital Rights Ireland*, *Schrems*, and *Tele2* shows its determination in affirming the fundamental rights to privacy and data protection in the face of claims by states regarding necessity in counter-terrorism measures. However, it is worth noting here that a closer look at the Court's Opinion elicits the question whether it is really a win for those fundamental rights. This is because, by contrast with its case-law, it did not voice its discontent with the 'general and indiscriminate retention'[119] of personal data, or on the mass surveillance of air passengers. In the view of the Court, the transfer of PNR data of all passengers regardless of their prior criminal record was justified because the objective of utilising PNR data automatically is to assess the risk a passenger possess for public security before the passenger concerned is admitted to the country. Therefore, the very nature of this objective did not require the link between the person and the risk on the ground of terrorism. Seen from another angle, the Court indirectly acknowledged that travelling per se

---

Preliminary Opinion on the agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences', (EDPS, 12 February 2016) available at <https://edps.europa.eu/sites/edp/files/publication/16-02-12_eu-us_umbrella_agreement_en.pdf> (accessed 29 November 2017).

[117] Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L 119/132.

[118] AccessNow, 'In win for privacy, European court rejects EU-Canada "PNR" agreement' (26 July 2017) Press Release available at <https://www.accessnow.org/win-privacy-european-court-rejects-eu-canada-pnr-agreement/> (accessed 29 November 2017).

[119] Tele2 (n 47), para. 112.

is such a link, intertwining measures of border control and of counter-terrorism.[120] This is certainly at odds with the Article 29 Working Party's and the EDPS's opinions on the PNR scheme, where both authorities denounced its feature of indiscriminate transfer, collection, and processing of data in bulks.[121]

Another point worth to mention is that the CJEU considered for the first time the automated decision-making and information retrieval from a voluminous amount of data. Although this consideration is welcoming, it is important not to lose sight of the fact that the discourse surrounding the pre-established models (i.e. algorithms) upon which automated decisions are reached are more complex than the Court touched upon. As an example, the Court noted that these models should be specific and reliable, but in many cases, the public authorities either have declined to provide information on these models by revoking the national security interest or have merely stated that they are reliable without any further detail on the matter. Also, the reasonable suspicion that the CJEU mentioned in identifying passengers who might participate in terrorist offences or transnational crimes through running algorithms against their PNR data might not be the same as the reasonable suspicion arrived at through observations, discrete facts, or limited information by law enforcement authorities because it consists of a search through vast networked information sources including a proxy for flagging the person as a reasonable suspect, which is previous convictions, previous arrests, or previous reports on participation in the offences concerned. Equally important is

[120] For the socio-political account of the intertwinement of border control and counter-terrorism see; Arjun Appadurai, 'Democracy fatigue' 1-12 in: Heinrich Geiselberger (ed.), *Great Regression*, (Polity Press, 2017).

[121] Article 29 Working Party recommended the transfer of PNR data on a case-by-case basis rather than in bulks. See; Article 29 Working Party, 'Opinion 7/2010' (n 59), 5-6. According to the EDPS, 'the non-targeted and bulk collection and processing of data of the PNR scheme amount to a measure of general surveillance.' See; Opinion 5/2015 of the European Data Protection Supervisor on Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, (EDPS, 24 September 2015) available at <https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf> (accessed 29 November 2017) note 68.

the margin of error that the automated decision-making presents. Having accepted a significant level of margin of error, the Court gave emphasis on the need not to have solely this mean of decision to adopt measures against individuals. However, the question relating to the margin of error should have been dealt in relation to the appropriateness of the processing of PNR data in countering terrorism and transnational crime because if the automated decision-making measure generates a significant level of error, it may be considered as useless to attain its objective.[122] Had the Court considered this point, the automated processing of PNR data might have been considered inappropriate for the purpose that processing pursues and the Agreement would have been considered as a violation of privacy and data protection rights, without having to delve into the proportionality of the Agreement.

Be that as it may, whilst the CJEU did not reject the PNR scheme as a whole, it provided a check-list of procedural requirements for that scheme to be compatible with EU fundamental rights. These requirements can be difficult to fulfil because each of them contains layers of discussions on their own. For example, the Court noted that the pre-established models (i.e. algorithms) must be specific, reliable, and non-discriminatory, but how this will be investigated is not an easy task. Therefore, the detail and the complexity that come with the procedural requirements might suggest that the Court might not have struck down the PNR data scheme altogether, but it sure has made it hard to design a EU fundamental rights complaint scheme.

[122] Bruce Schneier, 'Automated Targeting System' *Schneier on Security,* 22 December 2006, available at <https://www.schneier.com/blog/archives/2006/12/automated_targe.html> (accessed 29 November 2017).