Overviews

Opinion 1/15: The Court of Justice Meets PNR Data (Again!)

Table of Contents: I. Introduction. – II. Legal and factual background. – III. Opinion of AG Mengozzi. – IV. Opinion of the Court of Justice. – V. Analysis. – VI. Conclusion.

I. In July 2017 the Court of Justice handed down its eagerly awaited Opinion 1/15[1] on the compatibility of the envisaged EU-Canada Passenger Name Record (PNR) Agreement, that had been sought by the European Parliament.[2] The Court's careful analysis of the Agreement and its conclusion that it was not compatible with the Charter of Fundamental Rights of the European Union (Charter) is to be commended for continuing with the high level of privacy and data protection standards articulated in recent case-law. The ramifications of the Opinion are considerable. Steps are already afoot to renegotiate the Canada PNR Agreement to address the many concerns expressed by the Court of Justice in Opinion 1/15 so that this Agreement could eventually enter into force and potentially provide a template for all future PNR Agreements. Crucially the only existing PNR Agreements that are in force, with the US and Australia,[3] cannot be considered compatible with the standards articulated in Opinion 1/15 and are thus in need of renegotiation. This will be no small feat given the diverging approach to privacy and data protection in the US, to say nothing of the current US administration's more isolationist stance. Furthermore, it is submitted that the EU's own recently adopted General Data Protection Regulation[4] does not meet the standards articulated in Opinion 1/15 and will need revising.

[1] Court of Justice, opinion 1/15 of 26 July 2017.

[2] European Parliament Resolution P8_TA(2014)0058 of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data. The Canada PNR Agreement was signed on 25 June 2014.

[3] Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security; Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service.

[4] Regulation (EU) 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 (General Data Protection Regulation).

www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/176

II. PNR data is information provided by airline passengers and collected by air carriers to enable reservations to take place. This is an expansive category of data that can include, amongst other things, payment information, e-mail addresses, contact telephone numbers, passport information, baggage information, travel itinerary, frequent flier information, special health requirements and meal preferences (the latter category is considered particularly controversial due to its potential use as a proxy for ethnicity and religious beliefs).

PNR data gave rise to major transnational controversy when, in the immediate wake of the terrorist attacks on 11 September 2001, the US passed legislation requiring airlines flying into US territory to provide the Bureau of Customs and Border Protection with electronic access to PNR data. The failure of airlines to comply with these rules could lead to substantial fines and potentially even the loss of landing rights. Given the radically different approach to privacy and data protection taken by the US as compared to the EU,[5] the transfer of PNR data by airlines flying from Europe raised an obvious conflict with the Data Protection Directive which, subject to certain exceptions, only permits data transfers to a third country which "ensures an adequate level of protection".[6]

Negotiations ensued between the European Commission and the US that culminated in an international agreement that contained a range of commitments in relation to the PNR data and in a Commission finding that the US ensured an adequate level of data protection in relation to the PNR data.[7] The Council had concluded this EU-US PNR Agreement even though the European Parliament had sought an opinion from the Court of Justice, under what is currently Art. 218, para. 11, TFEU, as to the appropriate legal basis for the agreement and whether it was compatible with the right to protection of personal data.[8] The European Parliament accordingly withdrew its request under the opinion procedure and brought annulment proceedings against both the Adequacy Decision and the Decision concluding the PNR Agreement. Prior to the Court's ruling, another transatlantic PNR Agreement was concluded, this time with Canada and with clearly higher data protection standards than was the case in the EU-US Agreement as made clear in an opinion by the European Data Protection Supervisor (EDPS).[9] The Court itself was able to wholly avoid commenting on the compatibility of the EU-US PNR Agreement with fundamental rights standards by finding it to have been concluded

[5] See briefly on these differences: P.M. SCHWARTZ, *The EU-US Privacy Collision: A Turn to Institutions and Procedures,* in *Harvard Law Review*, 2013, pp. 1973-1979.

[6] Art. 25, para. 1, of 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 (Data Protection Directive).

[7] An Adequacy Decision under the Data Protection Directive.

[8] Registered as Court of Justice, opinion 1/04.

[9] 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, and the EDPS opinion (2005/C 218/06).

on the wrong legal basis.[10] The first EU-US PNR Agreement was then replaced with an *interim* third pillar agreement in 2006 with even lower data protection standards than its predecessor, and that in turn was replaced by another third pillar agreement in 2007 with yet lower standards.[11] In the immediate wake of the signing of the 2007 EU-US Agreement, a proposal for a third pillar EU wide PNR scheme for law enforcement purposes emerged which shared at least some disconcerting parallels with its EU-US counterpart, not least in relation to lengthy retention periods.[12]

The context for PNR schemes was transformed with the entry into force of the Lisbon Treaty in late 2009. PNR Agreements would now need, pursuant to Art. 218, para. 6, let. a), sub-let. v), TFEU, the European Parliament's approval and, as the Charter was now in force its specific provision on the right to the protection of personal data (Art. 8 of the Charter), as well as a nearly textually identical provision to that in Art. 8 of the European Convention on Human Rights (ECHR) concerning the right to respect for private and family life (Art. 7 of the Charter), would need to be complied with.[13] Notwithstanding this changed environment, the European Parliament still gave its approval to the latest iteration of the EU-US PNR agreements in 2012 despite the Agreement being riddled with data protection shortcomings.[14]

It would not be possible to remain as cavalier about the compatibility of PNR schemes with EU fundamental rights following the Court of Justice's seminal *DRI* ruling in April 2014, that invalidated the Data Retention Directive due to non-compliance with the Charter rights to private and family life and personal data protection.[15] Accordingly, the European Parliament relied on this ruling when invoking the Art. 218, para. 11, TFEU procedure in relation to a new PNR Agreement with Canada that was signed shortly after the *DRI* rul-

[10] Court of Justice, judgment of 30 May 2006, joined cases C-317/04 and C-318/04, *European Parliament v. Council and Commission*. See on this ruling, including criticism of the opinion of AG Léger delivered on 22 November 2005 that surprisingly found the US PNR Agreement compatible with the standards of Art. 8 ECHR: M. MENDEZ, *Passenger Name Record Agreement*, in *European Constitutional Law Review*, 2007, p. 127.

[11] See V. PAPAKONSTANTINOU, P. DE HERT, *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic*, in *Common Market Law Review*, 2009, p. 885; see also for criticism of the *interim* Agreement, M. MENDEZ, *Passenger Name Record Agreement*, cit., pp. 140-147.

[12] Commission Proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final. See for discussion including citations to criticism from the Article 29 Working Party, the European Parliament, the EDPS and the Fundamental Rights Agency: M. TZANOU, *The Fundamental Right to Data Protection*, Oxford: Hart Publishing, 2017, pp. 156-157.

[13] Art. 16, para. 1, TFEU, essentially replicates Art. 8, para. 1, of the Charter.

[14] See M. TZANOU, *The Fundamental Right to Data Protection*, cit., pp. 134-137.

[15] Court of Justice, judgment of 8 April 2014, joined cases C-293/12 and C-594/12, *Digital Rights Ireland* [GC]. For detailed discussion see O. LYNSKEY, *The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2014, p. 1789.

ing and then put to the Parliament for approval.[16] Nevertheless while Opinion 1/15, which is the focus of this *Overview*, was pending, Parliamentary approval was forthcoming for the EU's own controversial PNR scheme.[17] The EU's PNR Directive was passed in 2016,[18] notwithstanding a EDPS opinion, drawing on the *DRI* ruling, that found the proposal failed to satisfy the Charter, Art. 16 TFEU and Art. 8 ECHR, and which invited the legislator to wait for the ruling on the Canada PNR Agreement since "the answer of the Court may have a significant impact on the validity of all other PNR instruments".[19]

Before the Court of Justice itself came to deal with the Canada PNR Agreement it handed down two seminal rulings, drawing on its *DRI* ruling, which left little doubt that the Agreement could not emerge unscathed. In October 2015 the Grand Chamber's *Schrems* ruling invalidated the long-standing Adequacy Decision for the Safe Harbour Principles with the US whereby personal data transfers to US based companies were permissible where the companies had signed up to comply with a set of data protection principles.[20] Crucially the Court concluded that "an adequate level of protection" under Art. 25 of the Data Protection Directive required "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union" and "that review of the[se] requirements [...] should be strict".[21] This pointed to a higher threshold than might have been anticipated given that, as has been pointed out, when the Data Protection Directive was adopted the EU legislator had specifically preferred the term "adequate protection" over "equivalent protection".[22]

The second Grand Chamber ruling came in December 2016 in *Tele2/Watson* dealing with national data retention legislation.[23] The Court continued with the demanding privacy and data protection standards under the Charter that it had articulated in the *DRI* and *Schrems* cases and even set itself against "general and indiscriminate [data] reten-

[16] See footnote no. 2.

[17] The Directive was adopted in April 2016, the joint position having been agreed in December 2015, long after the Parliament had invoked the Art. 218, para. 11, TFEU procedure.

[18] Directive (EU) 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.

[19] EDPS, opinion 5/2015 of 24 September 2015 on the Canada PNR Agreement (2014/C 051/6).

[20] Court of Justice, judgment of 6 October 2015, case C-362/14, *Schrems v. Data Protection Commissioner* [GC]. For detailed commentary, see C. KUNER, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, in *German Law Journal*, 2017, p. 881.

[21] *Schrems* [GC], cit., para. 73.

[22] See C. KUNER, *Reality and Illusion*, cit., p. 899 (citing S. SIMITIS, U. DAMMANN, *EG-Datenschutzrichtlinie*, Baden-Baden: Nomos, 1997, p. 273).

[23] Court of Justice, judgment of 21 December 2016, joined cases C-203/15 and C-698/15, *Tele2 Sverige and Watson* [GC].

tion".[24] PNR schemes are arguably a form of general and indiscriminate data retention and the signs accordingly looked ominous for the Canada PNR Agreement.

III. The Advocate General's opinion on the Canada PNR Agreement emerged before the *Tele2/Watson* ruling.[25] He dealt first with the Parliament's second question which queried whether Arts 81, para. 1, let. d), and 87, para. 2, let. a), TFEU "constitute the appropriate legal basis for the act of the Council concluding the envisaged agreement or must that act be based on Article 16 TFEU?". AG Mengozzi concluded in light of the aim and content of the Agreement that it pursued two inseparably linked objectives, Canadian processing of passenger data for combatting terrorism and other serious transnational crime, and safeguarding the right to respect for privacy and the right to protection of personal data, and that it should accordingly have been based on Art. 16, para. 2, TFEU and Art. 87, para. 2, let. a), TFEU. On the Parliament's second question, whether the Agreement was "compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to protection of personal data?", the Advocate General in a detailed and careful analysis, that drew frequently on the *DRI* and *Schrems* rulings, concluded that it was indeed incompatible with these provisions of the Charter.[26]

IV. Like the Advocate General, the Court of Justice dealt first with the Parliament's second question concerning the appropriate legal basis and commenced by reiterating the standard line that the choice of legal basis "must rest on objective factors amenable to judicial review, which include the aim and content of that measure".[27] Following an assessment of both the aim and content of the envisaged Agreement, the Court in line with the Advocate General's opinion, concluded it had two inextricably linked components, "one relating to the necessity of ensuring public security and the other to the protection of personal data".[28] And like AG Mengozzi, the Court of Justice held that the Council Decision concluding the envisaged Agreement would have to be based jointly on Arts 16, para. 2, and 87, para. 2, let. a), TFEU.[29]

Turning to the second question, a detailed analysis resulted in the conclusion that the envisaged Agreement was incompatible with Arts 7, 8, 21 and 52, para. 1, of the

[24] *Ibid.*, para. 103.

[25] Opinion of AG Mengozzi delivered on 8 September 2016, opinion 1/15.

[26] *Ibid.* Curiously in dealing with this question, the Advocate General only referred to Art. 16 TFEU, when underscoring its second paragraph and the need for independent control (*ibid.*, para. 306).

[27] Opinion 1/15, cit., para. 76.

[28] *Ibid.*, paras 80-94.

[29] *Ibid.*, paras 95-118.

Charter,[30] the Court having first explained that it would not refer to Art. 16, para. 1, TFEU, as only Art. 8 of the Charter laid down in a more specific manner the conditions under which personal data may be processed. The Court unsurprisingly concluded that the transfer and processing of the PNR data, which included information on identified individuals, would interfere with the fundamental rights to respect for private life guaranteed by Art. 7 and the protection of personal data guaranteed in Art. 8 of the Charter. As with the Advocate General, the key issue turned on the justification for any such interference. The Court first rejected the Parliament's contention that the Agreement could not fall within the notion of "law" under Art. 8, para. 2, of the Charter, and therefore also Art. 52, para. 1, of the Charter, in that it did not constitute a "legislative act". Here the Court highlighted the symmetry between the procedure for adopting EU measures internally and international agreements in given fields, agreements thus being the equivalent externally of a legislative act internally, and the fact that it had not been argued that the Agreement might not meet the accessibility and predictability requirements to be regarded as being laid down by law for the purposes of Arts 8, para. 2, and 52, para. 1, of the Charter. The Court also accepted that the interferences entailed by the Agreement were capable of being justified by an objective of general interest of the EU, namely ensuring public security and the fight against terrorist offences and serious transnational crime, and were not "liable adversely to affect the essence of the fundamental rights enshrined in Articles 7 and 8 of the Charter".[31] The transfer of the PNR data to Canada and its subsequent processing was also regarded as being appropriate for achieving the objective of protecting public security and safety.

The Agreement fell short at the necessity hurdle, which required that the interferences were limited to what was strictly necessary and that the Agreement "lays down clear and precise rules governing the scope and application of the measures provided for".[32] Numerous shortcomings were identified with the Agreement in this respect. Firstly, the PNR data to be transferred was not sufficiently clearly and precisely defined. The Court took issue with three of the 19 PNR data headings.[33] In relation to heading 5, which refers to "available frequent flyer and benefit information (free tickets, upgrades, etc.)", the term "etc." was held not to "specify to the requisite standard the scope of the data to be transferred", nor was it clear from heading 5 whether it covered all information relating to air travel and transactions carried out in the context of customer loyalty programmes.[34] In relation to heading 7, the use of the terms "all available contact information" did not specify what type of contact information is covered nor whether it

[30] *Ibid.*, paras 119-231.

[31] *Ibid.*, para. 151.

[32] *Ibid.*, para. 154.

[33] Whilst other headings (8 and 18) could, if construed as outlined by the Court, be regarded as meeting the clarity and precision requirements (Opinion 1/15, cit., paras 159 and 161).

[34] Opinion 1/15, cit., para. 157.

also covered "the contact information of third parties who made the flight reservation for the air passenger, third parties through whom an air passenger may be contacted" or "who are to be informed in the event of an emergency".[35] Heading 17, which refers to "general remarks including Other Supplementary Information (OSI), Special Service Information (SSI) and Special Service Request (SSR) information", was considered to provide "no indication as to the nature and scope of the information to be communicated, and it may even encompass information entirely unrelated to the purpose of the transfer of PNR data", and because the information referred to in heading 17 was only listed by way of example, it set no "limitation on the nature and scope of the information that could be set out thereunder".[36] Crucially heading 17 was also problematic because sensitive data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information about a person's health or sex life"[37] could fall within its scope. And the risk of such data being processed contrary to the non-discrimination clause in Art. 21 of the Charter required "a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime" and there was no such justification.[38]

Secondly, the Court underscored the need for the automated processing of PNR data via pre-established models and criteria to be specific and reliable, making it possible to arrive at results targeting individuals under a reasonable suspicion of participation in terrorist offences or serious transnational crime, and non-discriminatory.[39] Any cross-checking of the PNR data would have to be limited to reliable and up to date databases used by Canada in the fight against terrorism and serious transnational crime. And any positive result obtained from automated processing must be subject to an individual re-examination by non-automated means before an individual measure adversely affecting air passengers is adopted.

A third deficiency concerned the purposes for which PNR data may be processed, notably the authorisation "on a case-by-case basis" in order to "ensure the oversight or accountability of the public administration" and to "comply with the subpoena or warrant issued, or an order made, by a court" (Art. 3, para. 5, let. a) and b), of the Agreement) which was considered too vague and general.[40]

A fourth shortcoming concerned the retention and use of PNR data. Here the Court distinguished between the retention and use of PNR data before the arrival of air passengers, during their stay and on their departure, as contrasted with after their departure. In relation to the former, the Court concluded that the retention and use of PNR

[35] *Ibid.*, para. 158.
[36] *Ibid.*, para. 160.
[37] As defined by Art. 2, let. e), of the Canada PNR Agreement.
[38] Opinion 1/15, cit., para. 165.
[39] *Ibid.*, paras 168-174.
[40] *Ibid.*, paras 175-179.

data of all passengers up to departure does not exceed the limits of what is strictly necessary as the necessary connection between the PNR data and security checks and border control checks exists. However, in relation to cases in which the Canadian Competent Authority has information collected during passengers' stay indicating that use of their data might be necessary to combat terrorism and serious transnational crime, rules laying down the substantive and procedural conditions governing use of that data are required and, except in cases of validly established urgency, should be subject to prior review either by a court or an independent administrative body. The Court concluding in this respect that "where there is objective evidence from which it may be inferred that PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious transnational crime, the use of that data does not exceed the limits of what is strictly necessary".[41]

In relation to the retention of the PNR data of all passengers after their departure from Canada, this was found not to be limited to what was strictly necessary as contrasted with specific cases in which "objective evidence is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada".[42] As with the use of such data in relation to the duration of a passengers stay, the Court underscored the need for such use to be based on objective criteria and, except in cases of validly established urgency, to be subject to a prior review by a court or independent administrative body.

A fifth problem concerned the disclosure of the data to both government authorities and individuals, neither of which was acceptable to the Court in the manner permitted by the Agreement. In relation to disclosure by the Canadian Competent Authority to other Canadian government authorities and government authorities of third countries, the Court underscored that this must comply with the conditions governing use of such data that it had outlined which included the rules based on objective criteria, objective evidence and, except in cases of validly established urgency, prior review by a court or independent administrative body. The Court also highlighted that the Agreement accorded "the Canadian Competent Authority a discretionary power to assess the level of protection guaranteed in [third] countries".[43] It reiterated the *Schrems* case holding that a transfer of personal data to a non-member country can only take place if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU. And that any disclosure required either an agreement between the EU and the third country or an adequacy decision under the Data Protective Directive. In relation to data disclosure to individuals, the Court was

[41] *Ibid.*, para. 201.
[42] *Ibid.*, paras 206-207.
[43] *Ibid.*, para. 213.

rightly troubled by the absence of constraints. It noted that the "agreement does not delimit the nature of the information that may be disclosed, nor the persons to whom such disclosure may be made, nor even the use that is to be made of that information", and underscored that there was no requirement that the disclosure "be linked to combating terrorism and serious transnational crime or that the disclosure be conditional on the authorisation of a judicial authority or an independent administrative body".[44]

In the penultimate section of the Opinion the Court found further failings in that to ensure that guarantees under Arts 7 and 8 of the Charter concerning access to personal data and the right to rectification were complied with, passengers must be individually notified of the transfer of their data to Canada and its use as soon as the information was no longer liable to jeopardise investigations being carried out by government authorities. Finally, and again in line with the Advocate General's opinion, the Agreement did not guarantee in a sufficiently clear and precise manner that oversight of compliance with its data protection rules would be carried out by an independent authority within the meaning of Art. 8, para. 3, of the Charter.

V. It was unsurprising that the Court found the Agreement wanting *vis-à-vis* the standards articulated in the Charter, as developed by the Court itself in its trilogy of rulings between 2014 and 2016 (*DRI*, *Schrems* and *Tele2/Watson*) and also in light of the Advocate General's opinion. It is noteworthy that, as recounted in the Advocate General's opinion, some governments had specifically argued for a limited scope of review and broader discretion for institutions for the adoption of an act forming part of the context of international relations.[45] This was given short shrift by the Advocate General and although not expressly commented on by the Court it clearly and rightly proceeded to adopt a rigorous standard of review and went through relevant provisions of the Agreement with something of a fine comb. Taking issue with "etc." in heading 5 might be thought to be a clear illustration of this. And one noted privacy expert has queried "how many international agreements of the EU could withstand this degree of second-guessing", suggesting that "some third countries may be hesitant to invest the time and resources necessary to conclude an international agreement on data protection with the EU knowing that it may later be picked apart by the Court".[46] There are a few points worth noting in this respect. It always seemed inevitable that there would be a considerable "degree of second-guessing" involved because we were dealing with an agreement that was negotiated prior to key jurisprudential developments. Indeed the key trigger for use of the opinion procedure was the *DRI* ruling. We might accordingly hope

[44] *Ibid.*, paras 216-217.

[45] *Ibid.*, paras 197-204.

[46] C. KUNER, *Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15*, in *Verfassungsblog*, 26 July 2017, verfassungsblog.de.

that future data protection related agreements will be sensitive to various key traits in the jurisprudence enunciated between the *DRI* ruling and Opinion 1/15, and it thus does not follow that future agreements would not withstand the scrutiny displayed in Opinion 1/15, nor as a result that countries should be hesitant to invest the time and resources to conclude them.

It is worth also reiterating the much repeated justification for the *ex ante* review procedure deployed since Opinion 1/75,[47] and underscored by the Court in Opinion 1/15 at paras 69 and 74, namely, to forestall complications that would arise from disputes concerning the compatibility with the EU Treaties of binding EU Agreements. In other words, the Court was dealing with an agreement that was not yet in force, and with appropriate political will changes could be made to it, matters are more complicated where instead a legal challenge takes place to an agreement that is already binding on the EU. In this sense we should be grateful for the presence of the opinion procedure which not only allows for review to take place, but allows it to take place in an arguably less charged political setting than would be the case if we were to allow exclusively *ex post* type review.[48] It can, however, be argued that this is all well and good, one can be supportive of the opinion procedure in principle, but contest instead the demanding standards for international data transfers being deployed by the Court. However, as the Court already made clear in *Schrems* when first articulating the essential equivalence standard in the level of fundamental rights protection, to do otherwise would disregard the Data Protection Directive purpose of ensuring a high level of data protection where personal data is transferred to a third country. Indeed the elements to be taken into account in an adequacy assessment have if anything become more demanding under the General Data Protection Regulation, which was itself shaped by the *Schrems* ruling.[49] Thus rather than criticise the Court for its detailed scrutiny of the Canada PNR Agreement, we should praise it for seeking to ensure that the privacy and data protection standards in the Charter are taken seriously and that, despite the very real threat of terrorism and serious crime, international agreements cannot simply be used in a manner that rides roughshod over these fundamental rights. The Court of Justice is in a privileged position in this respect, as the Constitutional Court for a politically and economically powerful organisation. It is well known that EU data protection law, and particularly the constraints on international data transfers under the Data Protection Directive, have served to shape and increase data protection standards in many other countries and even to some extent in a reluctant United States with its very different privacy philosophy.[50]

[47] Court of Justice, opinion 1/75 of 11 November 1975.

[48] See also M. MENDEZ, *Constitutional Review of Treaties: Lessons for Comparative Constitutional Design and Practice*, in *International Journal of Constitutional Law*, 2017, p. 84, making the case for constitutional systems to deploy both *ex ante* and *ex post* constitutional review of treaties.

[49] Art. 45, para. 2, of Regulation 2016/679, cit.

[50] See briefly A. BRADFORD, *The Brussels Effect*, in *Northwestern University Law Review*, 2012, pp. 22-26.

Opinion 1/15 is to be welcomed to the extent that it bolsters the aforementioned dynamic in a manner that constrains measures of "pre-emptive surveillance".[51]

An alternative line of criticism would be to suggest that in fact Opinion 1/15 might not go far enough. We have seen that the Court accepted that the Agreement does not "exceed the limits of what is strictly necessary merely because it permits the systematic retention and use of the PNR data of all air passengers".[52] And yet PNR schemes do *prima facie* seem to fall within the remit of the "general and indiscriminate [data] retention" with which the Court took issue in *Tele 2/Watson* and Opinion 1/15 does not actually make clear how the general and indiscriminate retention of PNR data is different. As Woods noted, the difference may be in the nature of the data but, even if this is so, the Court does not make the argument and rather weakly accepts the need for the data.[53] The EDPS would surely have expected more by way of justification given that it has consistently underscored that it "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".[54] In short, we can also expect criticism of Opinion 1/15 for essentially giving the green light to PNR schemes, subject to certain significant safeguards and constraints being in place. Perhaps this is the most that can have realistically been expected given the rapid and growing deployment of PNR schemes, including crucially within the EU itself, especially in light of access to PNR data becoming a central aspect of the US's counter terrorism strategy since 11 September 2001. Put another way, the PNR ship is one that has already sailed both outside and now also within the EU, and a full on assault on PNR schemes, as contrasted with shaving off some of the worst excesses, thus always seemed unlikely.

Turning now to the immediate ramifications of Opinion 1/15, firstly and most obviously it means that the Agreement will need significant revisions before it can be concluded.[55] Already by October 2017 the Commission had submitted a recommendation to the Council to authorise the opening of negotiations for a revised Agreement,[56] a recommendation which noted that Canada had expressed its wish to enter negotiations

[51] See on the new era of pre-emptive surveillance, V. MITSILEGAS, *The Transformation of Privacy in an Era of Pre-Emptive Surveillance*, in *Tilburg Law Review*, 2015, p. 35.

[52] Opinion 1/15, cit., para. 197.

[53] L. WOODS, *Transferring Personal Data Outside the EU: Clarification from the ECJ?*, in *EU Law Analysis*, 4 August 2017, eulawanalysis.blogspot.co.uk.

[54] EDPS, opinion 5/2015 of 24 September 2015 on the Canada PNR Agreement (2014/C 051/6).

[55] Art. 218, para. 11, TFEU expressly stipulates "[w]here the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised". The Treaties have never been revised to accommodate an adverse opinion (unless we include the addition of Art. 6, para. 2, TEU as a belated response to Court of Justice, opinion 2/94 of 28 March 1996).

[56] Recommendation for a Council Decision authorising the opening of negotiations on an Agreement between the European Union and Canada for the transfer and use of Passenger Name Record (PNR) data to prevent and combat terrorism and other serious transnational crime, COM(2017) 605 final.

again to find mutually acceptable terms consistent with the Court's findings. Opinion 1/15 also had implications for existing negotiations on PNR Agreements, thus Mexico, with which negotiations on a PNR Agreement had commenced in 2015, was informed by the Commission that negotiations could not be finalised until Opinion 1/15 had been delivered.[57] The Commission had also made clear in 2015 that once Opinion 1/15 was issued it would "finalise its work on legally sound and sustainable solutions to exchange PNR data with other third countries, including by considering a model agreement on PNR setting out the requirements third countries have to meet to receive PNR data from the EU".[58] A revised Canada PNR Agreement may well provide the basis for a model PNR Agreement given that the new negotiations are precisely about ensuring compliance with the standards articulated in Opinion 1/15.

The second obvious ramification of Opinion 1/15 concerns the two existing PNR Agreements with respectively the US and Australia. The focus here is on substantive compatibility, however, both Agreements suffer from the same legal basis problem as the Canada PNR Agreement because they are also based on Arts 82, para. 1, let. d), and 87, para. 2, let. a), TFEU. Both Agreements are clearly incompatible with the standards enunciated in Opinion 1/15 which should be wholly unsurprising given that like the Canada Agreement they also predate the case-law developing the Charter standards in this respect that began with the 2014 *DRI* ruling. It is only necessary here to highlight a few of these shortcomings by analogy with those found *vis-à-vis* the Canada Agreement to demonstrate the incompatibility. Firstly, both Agreements are based on exactly the same PNR data headings as in the Canada Agreement, which as the Court noted correspond to the Guidelines of the International Civil Aviation Organisation on PNR data.[59] In this respect, the US and Australia Agreements will both fall foul of the requirement that the PNR data to be transferred be sufficiently clearly and precisely defined (specifically because of headings 5, 7 and 17). The Australia Agreement does however contain an express prohibition on the processing of sensitive data,[60] which the Advocate General had underscored as suggesting that the Canada Agreement's objectives could be attained just as effectively without any sensitive data being transferred. Whilst we have seen that the Court itself did not rule out transfers of sensitive data, it did require a "precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime" which would thus

[57] See the Commissioner response of 5 October 2015 to MEP question E-009612/15 of 11 June 2015.

[58] Communication COM(2015) 185 final from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *The European Agenda on Security*.

[59] See the annexes to all three Agreements.

[60] Art. 8, and also a provision on the deletion of any such data that is transferred: Art. 15, para. 2. The EDPS opinion (2011) on the proposal pointed out that the sending of any such data by "airlines is an act of processing [… and] that the airlines should be obliged to filter sensitive data at the source of the processing".

certainly catch the US Agreement. Indeed, the Court highlighted that the EU's own PNR Directive prohibited the processing of sensitive data, which suggests a very high threshold would need to be met to justify the transfer of such data in PNR Agreements.[61]

Secondly, there are purpose limitation shortcomings in the PNR Agreements. The Australia Agreement might well be satisfactory in relation to "terrorist offences" and "serious transnational crime" (as defined in Art. 3, paras 2 and 3) and processing of PNR data "[i]n exceptional cases [...] for the protection of the vital interests of any individual" (Art. 3, para. 4), given the similarity with the Canada PNR Agreement (Art. 3, para. 4) in this respect. But there is a not dissimilar provision to Art. 3, para. 5, of the Canada Agreement concerning processing of PNR data on a case-by-case basis for oversight and accountability of the public administration that was found wanting in terms of clarity and precision.[62] If the Canada Agreement was found wanting in this respect, there is no way that the US Agreement could be acceptable. It includes not just terrorist offences but also other "related crimes"; transnational crimes are extremely broadly defined (see Art. 4, para. 1); PNR data may also be "processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court" (Art. 4, para. 2), and may also be used and processed "to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination" (Art. 4, para. 3). If paras 2 and 3 of Art. 4 of the US Agreement do not alone demonstrate a relative absence of meaningful purpose limitations here, para. 4 proceeds to stipulate that "[p]aragraphs 1, 2, and 3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR".

Thirdly, in relation to the retention of PNR data, the Agreements do not of course distinguish between the retention of PNR data before arrival, during the stay of passengers and on their departure, on the one hand, and after their departure on the other, as the Court is requiring in Opinion 1/15, nor do they provide for the substantive and procedural constraints on use of such data that were outlined by the Court. The Australian retention period of five and a half years (Art. 16 of the Australia Agreement) might be thought not especially objectionable in light of the five years retention period of the Canada Agreement having been found not to "exceed the limits of what is strictly necessary for the purposes of combatting terrorism and serious transnational crime".[63] But it is hard to believe that the Court could ever accept as strictly necessary the 15 years

[61] Opinion 1/15, cit., para. 166.

[62] Art. 3, para. 5, of the Australia PNR Agreement.

[63] However, the Canada PNR Agreement provided for masking of the names of all passengers 30 days after Canada receives them (Art. 16, para. 3), whereas the Australia Agreement only provides for masking of data after three years (Art. 16, para. 1, let. b)).

retention period outlined in Art. 8 of the US Agreement, not least when one considers that the EU's PNR Directive has a five years retention period (Art. 12).

Fourthly, both Agreements provide for the transfer of PNR data to third country authorities,[64] and following the logic of the Court in Opinion 1/15 such disclosure would require an agreement between the EU and the third country or an adequacy decision under the Data Protection Directive. And as far as oversight of PNR data protection authorities is concerned, this would be particularly problematic under the US Agreement where pride of place is given to the Department for Homeland Security (DHS) "privacy officers, such as the DHS Chief Privacy Officer".[65] This is most unlikely to satisfy the independence threshold used by the Court of Justice given that the DHS is the very authority to which the data is transferred under the PNR Agreement.[66]

Clearly there is no difficulty in establishing that the two existing PNR Agreements do not meet the privacy and data protection standards outlined in Opinion 1/15. They have long been in force and so annulment actions are no longer a possibility.[67] However, a challenge could still take place domestically with a view to a preliminary ruling on the validity of these Agreements.[68] Such proceedings would take years and even if successful one would expect the Court to maintain in force the decisions concluding these PNR Agreements to take place; when the Parliament succeeded in annulment proceedings in relation to the first EU-US PNR Agreement it was the separate adequacy decision that was preserved.[69] The Agreements are based on a seven year duration from their entry into force in mid 2012, however, they automatically renew in the absence of a notice of intention not to renew being sent by either party at least 12 months before the expiry of the seven year period.[70] It is clearly now up to the Commission to seek to renegotiate these two PNR Agreements in light of the Opinion 1/15 findings and for them to be terminated in line with their provisions if this is not possible.[71] Indeed, if the Commission does not pursue a renegotiation of these Agreements, a challenge for a failure to act under Art. 265 TFEU would be conceivable.

[64] Art. 17 of the US Agreement, Art. 19 of the Australia Agreement.

[65] Art. 14, para. 1, of the US Agreement.

[66] See further F. Boehm, M.D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, 2014, p. 64, www.janalbrecht.eu.

[67] Art. 263, para. 6, TFEU.

[68] For a pending example of a preliminary ruling involving challenges to EU Agreements, see Court of Justice, case C-266/16, *Western Sahara Campaign UK*, in which the Court is being asked questions as to the validity of an Association Agreement with Morocco and a Fisheries Agreement with Morocco.

[69] See generally on how the CJEU has dealt with challenges to concluded EU Agreements including the first EU-US PNR Agreement, M. Mendez, *The Legal Effects of EU Agreements: Maximalist Treaty Enforcement and Judicial Avoidance Techniques*, Oxford: Oxford University Press, 2013, pp. 76-93.

[70] Art. 26 of both Agreements.

[71] Art. 25 of both Agreements stipulates that termination takes effect 120 days after notification or as the parties otherwise agree.

Opinion 1/15 will not however only be of relevance to international data transfers via PNR Agreements. The Safe Harbour replacement, the EU-US Privacy Shield that came into effect in August 2016, is currently the subject of annulment actions.[72] One would expect heavy reliance by the applicants on Opinion 1/15 not least in relation to onward transfers to third countries, the issue of effective remedies, and the independence of the newly created Privacy Shield Ombudsperson.[73]

Finally we must consider the ramifications of Opinion 1/15 for the EU's own PNR regime. The Advocate General rightly made clear that how the Court answered the questions before it would necessarily also have implications for the EU's PNR system. There are at least two particularly obvious shortcomings with the PNR Directive in light of Opinion 1/15. Firstly, although a number of the 19 data headings are phrased differently from the Canada Agreement, the reference in data heading 12 to "General remarks" corresponds to data heading 17 of the Canada PNR Agreement with which the Court took issue. Thus one can equally say that heading 12, as the Court held in relation to heading 17, provides "no indication as to the nature and scope of the information to be communicated, and it may even encompass information entirely unrelated to the purpose of the transfer of PNR data", and because the information referred to in heading 12 was only listed by way of example (it stipulates "including all available information on unaccompanied minors under 18 years"), it sets no "limitation on the nature and scope of the information that could be set out thereunder".[74] Secondly, and much more significantly, the PNR Directive does not of course distinguish, as required by Opinion 1/15, between the retention of PNR data before arrival, during the stay of passengers and on their departure, on the one hand, and after their departure, on the other.

The time-limit for annulment proceedings against the PNR Directive has now passed, but as with the two existing PNR Agreements, a domestic challenge leading to a preliminary ruling would be possible. Given the obvious implications of Opinion 1/15 for the PNR Directive one would, however, expect the Commission to prioritise taking steps towards a revision of the Directive particularly as third countries will need to be asked to meet certain standards pertaining to PNR Agreements that the EU's own regime does not yet meet.

VI. Opinion 1/15 is to be welcomed for continuing with the high privacy and data protection standards that the Court had articulated in the seminal earlier trilogy of cases (*DRI*, *Schrems* and *Tele2/Watson*). Crucially it is also to be welcomed for the Court showing,

[72] General Court: case T-670/16, *Digital Rights Ireland v. Commission* and case T-738/16, *La Quadrature du Net v. Commission*, both still pending.

[73] Points of controversy, amongst many others, already raised in the opinions by the EDPS (4/2016) and the Article 29 Working Party (01/2016) on the EU-US Privacy Shield draft Adequacy Decision, as well as more recently by the European Parliament: European Parliament Resolution P8_TA(2017)0131 of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield.

[74] Opinion 1/15, cit., para. 160.

as it has had occasion to do previously in *Schrems*, that it will not allow the EU's bilateral relations with other States to be used to simply ride rough shod over fundamental rights.[75] To be sure, for some the Court will not have gone far enough in that it essentially gives the green light to PNR schemes subject to certain constraints and safeguards, but for others it will have probed the substance of an agreement in excessive detail with troublesome consequences for the EU's international relations. It remains to be seen whether the Commission will be able to persuade third States of the need to meet the high standards set out in Opinion 1/15, the US will no doubt be the hardest to persuade given its diverging approach towards privacy. But, in any event, the EU's PNR Directive will not be able to remain wedded to lower standards than those outlined in Opinion 1/15. Whether we are dealing with the EU's internal PNR scheme or PNR Agreements with third countries, it will be a particularly formidable challenge to devise schemes that are able to give effect to the Court's proposed distinctions relating to the retention and use of PNR data before the arrival of air passengers, during their stay and on their departure, and after their departure.

Mario Mendez*

[75] A cautionary note has however been sounded as to the capacity to deliver on the high standards proclaimed, thus Kuner argued, while commenting on *Schrems* [GC], cit., that EU data protection law "maintains the illusion that it can provide seamless effective protection of EU personal data transferred around the world": C. KUNER, *Reality and Illusion*, cit., pp. 884-885.

* Reader in Law and Co-Director of the Centre for European and International Legal Affairs, Queen Mary University of London, mario.mendez@qmul.ac.uk.