To the President and Members of the Court of Justice of the European Union

OPINION 1/15

REPLIES OF IRELAND TO THE COURT'S QUESTIONS

Submitted by Eileen Creedon, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service via e-curia, assisted by David Fennelly BL.

Ireland has the honour to submit the following replies to the Court's questions to the parties dated 5th February 2016 in these proceedings, the subject of a request for an Opinion pursuant to Article 218(11) TFEU lodged by the European Parliament at the Court Registry on 30 January 2015.

***

1. Article 4 of the draft agreement provides that the EU is to ensure that air carriers are not prevented from transferring PNR data to the Canadian competent authority and Article 5 provides that that authority is deemed to provide an adequate level of protection, within the meaning of relevant EU data protection law, for the processing and use of PNR data. Does the guidance derived from the judgment in *Schrems*, C-362/14, EU:C:2015:650, apply *mutatis mutandis* to the assessment of the compatibility of the draft agreement with the Charter?

The transfer of PNR data to the Canadian Competent Authority under the draft agreement (**'the Agreement'**) does not as such fall within the scope of Directive 95/46/EC.[1] As a result, it is not subject to the specific regime for transfers of personal data to third countries laid down in Article 25 of the Directive which was the subject of the Court's judgment in *Schrems*. Nevertheless, the judgment in *Schrems* provides important guidance on the assessment of the adequacy of the level of protection for personal data in third countries for the purposes of EU law.[2] As Article 5 of the Agreement defines the concept of "adequate level of protection" by reference to EU data protection law, it is thus relevant for the assessment of the compatibility of the Agreement with the Charter.

[1] Judgment in *Parliament v. Council*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56.
[2] See also Article 13 of Council Framework Decision 2008/977/JHA.

In *Schrems*, this Court clarified that, while an adequate level of protection cannot require an identical level of protection for personal data in a third country, it "must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union…".[3] At the same time, the Court recognised that "the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection may differ from those employed within the European Union".[4]

In considering the adequacy of the level of protection provided under the Agreement in light of *Schrems,* Ireland makes the following observations. First, while Article 25(1) and 25(6) of the Directive specifically required a finding that a third country as such ensured an adequate level of protection,[5] EU law does not preclude a more limited finding of adequacy in respect of a third country authority in appropriate circumstances, as is the case in Article 5 of the Agreement. Secondly, as regards the *form*, in contrast to the Commission Decision 2000/520/EC at issue in *Schrems*, the Agreement, once concluded, would constitute a binding international agreement containing significant safeguards for the protection of personal data, supplemented where appropriate by the protections of Canadian domestic law. Thirdly, as regards the *substance*, by strictly restricting the scope of, use of and access to the relevant personal data and by imposing a series of effective safeguards against abuse, the Agreement offers a much high level of protection of personal data than applied under the regime deemed adequate in Commission Decision 2000/520/EC.

2. If, pursuant to Article 29 of the draft agreement, Denmark, Ireland or the United Kingdom are not party to the agreement, what would be the practical consequences, in particular in respect of the potential of the planned agreement to meet its objectives?

If Denmark, Ireland or the United Kingdom were not parties to the Agreement, this would limit the scope of the Agreement and, to some extent, its full effectiveness. The Agreement would apply between Canada and less than the full 28 Member States of the European Union. This would reduce the sphere of application of the key provisions of the Agreement on international cooperation, in particular through information-sharing. While Member States not parties to the Agreement would nonetheless be bound to comply with Canadian law on the provision of PNR data insofar as their air carriers fly to Canada, they would do so without the benefit of the

[3] Judgment in *Schrems*, C-362/14, EU:C:2015:650, paragraph 73.
[4] Judgment in *Schrems*, EU:C:2015:650, paragraph 74.
[5] Judgment in *Schrems*, EU:C:2015:650, paragraphs 96-97.

common framework provided for by the Agreement, including its data protection framework. Nevertheless, even if those Member States were not parties to the Agreement, it would still have very broad application across the EU and would provide an important common framework for PNR transfers for the vast majority of EU Member States. While non-participation of Denmark, Ireland or the United Kingdom might limit the scope of the Agreement, it would not be such as to undermine its appropriateness, effectiveness or utility.[6] It should of course be noted that Ireland and the United Kingdom have notified their wish to take part in the Decision approving the Agreement while Denmark has indicated that it is not taking part in the Decision.[7] In practical terms, this means that the Agreement would apply between Canada and 27 out of 28 Member States and would have almost universal coverage insofar as the EU is concerned.

3. According to settled case-law of the Court of Justice, the right to respect for private life requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.

a. According to publicly available information, under Canadian immigration rules, entry into Canada for the purposes of a temporary stay is subject to prior acquisition of either a visa or, as from 15 March 2016, an electronic travel authorisation. To that end, do the Canadian authorities collect personal data in respect of persons travelling by air from the EU to Canada before or at the time of their entry into that country, such that those persons and information concerning them can be identified? If so:

- What personal data is collected?

- As regards the objective of the draft agreement, what is the added value of the PNR data collected by air carriers for commercial purposes compared with the data collected by the Canadian authorities themselves, under Canadian law?

The data collected as part of the visa application and electronic travel authorisation process is collected by Citizenship and Immigration Canada ('**CIC**'), the Canadian immigration ministry. This data is collected and stored for immigration purposes. On the other hand, PNR data is collected for law enforcement purposes and is collected by the Canadian border control and customs agency, Canadian Border Services Agency ('**CBSA**'). CIC is a Government Ministry in Canada and reports to the Minister for Immigration, Refugees and Citizenship. The CBSA is a component law

[6] See, by analogy, judgment in *Digital Rights Ireland, Seitlinger & Others,* Joined Cases C-293/12 and C-594/12, EU:C:2014:238, paragraph 50.

[7] Draft Council Decision on the Conclusion on behalf of the Union of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, recitals 4 and 5.

enforcement agency of the Canadian Public Safety Ministry and as such reports to the Minister for Public Safety and Emergency Preparedness.

The Canadian authorities collect personal data in respect of persons travelling by air from the EU to Canada before or at the time of their entry into the country for immigration and border control purposes. The personal data collected varies according to the status of the person in question and the basis on which they are seeking to enter Canada. As part of the electronic travel authorisation a person's name, date of birth, country and city of birth, nationality or nationalities, funds available for stay in Canada, passport information (including passport number, place of issue, date of issue, date of expiry), e-mail and residential address is required to be submitted electronically by non-Canadians. Similar data would be collected for visa required applicants in order that immigration applications can be processed. It should be noted that this information is collected by CIC and is expressly collected for immigration purposes. It is collected for all migrants and foreign national travellers to Canada irrespective of their method of transport to Canada. In contrast, PNR data is collected on all passengers (including Canadian citizens) who are travelling by air to Canada**.** While there may be some overlap between the information collected by the Canadian authorities for this purpose and the PNR data collected by airlines and transferred to the Canadian Competent Authority, they are distinct sets of information collected for distinct purposes. The value added of PNR data lies not only in the fact that it contains additional information but also in the uses to which this data can be put, in particular though the various methods of analysis of PNR data which have been developed. The CSBA considers that such data, and the analysis that can be carried out thereon, are critically important in asessing threats of terrorism and serious transnational crime, a view shared by an increasing number of EU Member States and now recognised by the EU legislature.[8] In addition, the collection of data by the immigration authorities and of the PNR data by air carriers may, in appropriate cases, allow for cross-checking and verification of information.

b. The draft agreement provides for the transfer and use of PNR data from all air passengers travelling between the EU and Canada without any differentiation, limitation or exception being made in the light of the objective pursued. What is the specific relationship between the collection and retention of

[8] Within the EU, Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, Hungary, Latvia, Lithuania, the Netherlands, Portugal, Romania, Slovenia, Spain and the United Kingdom have established or in the process of establishing a national PNR system. The value of PNR analysis has been recognised at EU level. On 4 December 2015 the European Council approved the compromise text agreed with the European Parliament on the proposal for a Directive on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

the PNR data listed in the annex to the draft agreement and the objective pursued by that draft agreement? To what extent does PNR data allow air passenger profiles to be established? Can it be said that the draft agreement is limited to what is strictly necessary?

The PNR data listed in the annex to the draft agreement reflects the internationally recognised data ordinarily included in a PNR record.[9] An increasing number of States in the international community have developed techniques for the analysis of this PNR data which have been proven to provide significant assistance in the fight against terrorism and serious transnational crime, including drug trafficking, human trafficking and child abduction.[10] These techniques draw on the use of both historic and real-time PNR and have special value in identifying patterns of behaviour of concern and persons involved in serious crime who are not otherwise known to authorities. There is thus a close and established relationship between the collection and retention of PNR data and ensuring public security and safety through the combatting of terrorism and serious transnational crime. While PNR data may in some cases be used to establish air passenger profiles (for example, in the case of checks against known watch-lists), it is not systematically used for this purpose and the use of masking and depersonalisation techniques militate against such use. Instead, it draws on a much broader range of analytical tools to assist in the detection, prevention, investigation and prosecution of terrorism and serious transnational crime. While some elements of a PNR record may prove more useful than others in the detection, prevention, investigation and prosecution of terrorism and serious transnational crime, in Ireland's view, there is a value in maintaining the integrity of the record, particularly in circumstances where it is progressively masked or depersonalised. Having regard to the relatively discrete nature of PNR data, the very important purposes for which it is retained and used, and the significant safeguards imposed on access and use, Ireland submits that the Agreement is strictly limited to what is necessary to ensure public security and safety through the combatting of terrorism and serious transnational crime.

c. What provisions of EU law are used to assess the lawfulness of PNR data collection by air carriers for commercial purposes in the territory of the EU, including, inter alia, collection of the sensitive data referred to in the draft agreement.

[9] See, in this regard, International Civil Aviation Organization, *Guidelines on Passenger Name Record (PNR) Data* (2010).

[10] See, for example, the examples provided by the United Kingdom in its Written Observations, paragraphs 8-10.

As this Court has indicated in its judgment in Joined Cases C-317/04 and C-318/04, collection of PNR data by air carriers for commercial purposes in the territory of the EU may be considered as falling within the scope of Directive 95/46/EC.[11] Article 8 of Directive 95/46/EC governs the process of special categories of data, including sensitive data such as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".

4. As regards access to personal data by public authorities and its subsequent use by those authorities, the case-law of the Court requires that the rules in question lay down the relevant substantive and procedural conditions. Access to the data in question and its subsequent use must be strictly limited to specifically defined purposes capable of justifying the interference which both access to that data and its use entail. In particular, the Court required that access by a competent national authority to the data in question should be dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and its use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities.

a. Are air carriers required, in law and in practice, to provide access to PNR data automatically or solely at the request of the Canadian competent authority?

The domestic legal framework obliging air carriers to provide PNR data to the Canadian Competent Authority is to be found in the Canadian Customs Act and the Immigration and Refugee Protection Act and regulations made thereunder.[12] In accordance with Article 20 of the Agreement, air carriers transfer PNR data to the Canadian Competent Authority exclusively on the basis of the push method – that is, carriers transfer the data into the database of the requesting authority – and in accordance with the technical and security procedures laid down therein. As appears from Article 21 of the Agreement, the Canadian Competent Authority may require an air carrier to transfer PNR data on a scheduled basis (with the earliest point being up to 72 hours before scheduled departure) and a maximum of five times for a particular flight. Article 21(3) makes provision for requests for additional access in order to respond to a specific threat of terrorism or serious transnational crime. Subject to the

[11] Judgment in *Parliament v. Council*, C-317/04 and C-318/04, EU:C:2006:346, paragraph 57.

[12] See, in particular, the Customs Act, section 107.1; the Passenger Information (Customs) Regulations; Immigration and Refugee Protection Act, paragraph 148(1)(d), and the regulations made thereunder (including Immigration and Refugee Protection Regulations, regulation 269, and the Protection of Passenger Information Regulations).

Canadian Competent Authority notifying the air carriers of its requirements in this regard, Ireland understands that PNR data is thereafter transferred automatically.

b. To what extent may it be said that the draft agreement, and in particular Article 3(1) and (5) thereof, strictly limits access to PNR data and its subsequent use for precisely defined purposes capable of justifying the interference which both access to that data and its use entail?

In Ireland's view, Article 3 of the Agreement strictly limits access to PNR data and its subsequent use to precisely defined purposes capable of justifying the interference which access and use entail. Article 3(1) imposes a binding obligation on Canada to ensure that the Canadian Competent Authority, which has been designated as the Canada Border Services Agency, processes PNR data "strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime". Article 3(2) and Article 3(3) clearly define the concepts of "terrorist offence" and "serious transnational crime". In addition, Canada has furnished a non-exhaustive list of offences referred to in Article 3(3) of the Agreement. It is clear that Article 3 applies only to the most serious criminal offences, many of which represent the implementation of international obligations by which both Canada and EU Member States are bound. While Article 3(5) of the Agreement permits processing for two additional purposes, this is strictly on a case-by-case basis, for legitimate purposes of ensuring oversight or accountability of public administration and of complying with court orders, subpoenas or warrants and indeed may be considered as forming part of an overall effective framework for ensuring the accountability of the Canadian Competent Authority in its processing of PNR data in accordance with Article 3(1) and, more generally, as providing legal certainty in the use of such data.

c. To what extent may it be said that the draft agreement fulfils the requirements arising from the case-law of the Court of Justice referred to above, relating to the substantive and procedural conditions of access to personal data and its subsequent use by public authorities?

In Ireland's view, the Agreement fulfils the requirements arising from the Court's judgments in *Digital Rights Ireland* and *Schrems* relating to the substantive and procedural conditions of access to personal data and its subsequent use by public authorities. First, as Ireland has submitted at paragraph 15 of its Observations, the Agreement stands in sharp contrast to the Data Retention Directive, at issue in *Digital Rights Ireland*, by strictly restricting use of PNR data to the purposes laid down with precision in Article 3 of the Agreement. Secondly, as noted at paragraph 16 of the

Observations, Article 16(2) requires Canada to restrict access to a limited number of specially authorized officials and Article 18 places clear restrictions on further disclosure. Thirdly, the overall structure and purpose of the Agreement, and the in-built limits on the data transferred, its access and its subsequent use, are such that making access dependent on a prior review by a court or independent administrative authority would be neither practical nor appropriate. Fourthly, insofar as the retention period is concerned, Ireland refers to paragraph 18 of its Observations and its reply to Question 5 below.

5. What are the objective criteria which allow the Court to assess whether the five-year data retention period, provided for in Article 16 of the draft agreement, is limited to what is strictly necessary? In particular, the parties are requested to specify the objective criteria for considering that PNR data must be retained beyond the period of the planned stay of persons who have travelled by air from the EU to Canada.

In assessing whether the retention period of five years, provided for in Article 16 of the Agreement, is limited to what is strictly necessary, Ireland submits that the following objective criteria should be considered. First, it is clear that the fight against terrorism and the fight against serious transnational crime are among the most pressing challenges facing EU Member States and the international community in ensuring public security and safety. Secondly, terrorism and serious transnational crime, which by their nature frequently defy borders and traditional methods of criminal investigation, present particular difficulties for law enforcement. As a result, criminal investigations and prosecutions in these fields tend to be far more complex and to last significantly longer than investigations and prosecutions into other crimes. In the course of negotiations, Canada stated that, on the basis of its experience to date, the retention period of 3.5 years under the earlier agreement was a significant impediment to the effective use of PNR data because it is often only after a significant period of investigation into terrorist or criminal networks that a terrorist or serious criminal threat may be identified. It is on this basis, in light of the practical experience in the use of PNR data, that the retention period has been extended to a period of 5 years in the Agreement. This is the principal reason why it is necessary to retain the data beyond the period of the planned stay of persons who have travelled by air from the EU to Canada. If retention were limited to such a period, this would significantly undermine the effectiveness of PNR data for the purposes of fighting terrorism and serious transnational crime. Thirdly, one of the strengths of PNR data is that it can be used be in a range of ways – combining reactive, real time and proactive approaches –

which can add significant value to the process of criminal investigation.[13] Fourthly, and finally, while the retention period has been extended to a period of 5 years in the Agreement, this is subject to significant safeguards insofar as personal data is progressively masked or de-personalised.[14]

6. Article 10 of the draft agreement provides for oversight by 'an independent public authority, or by an authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy' .

Does the latter option imply that oversight may be carried out by an authority which is not independent within the meaning of the case-law of the Court? If so, to what extent does the requirement, laid down in Article 8(3) of the Charter and Article 16(2) TFEU, in relation to the establishment of independent supervisory authorities, apply in the event of the transfer of personal data from the EU to third countries?

The Court's case-law on the independence of supervisory authorities has developed within the context of the Member States' supervisory authorities whose establishment is envisaged in Article 28 of Directive 95/46/EC and which are required to "act with complete independence in exercising the functions entrusted to them".[15] As this Court has confirmed in *Schrems*, while national supervisory authorities have jurisdiction over the transfer of personal data from Member States to a third country, they do not have powers in respect of processing of such data carried out in a third country.[16] Thus, the requirement, laid down in Article 8(3) of the Charter and Article 16(2) TFEU does not, in a strict sense, apply to supervisory authorities in third countries. However, European Union law only permits the transfer of personal data outside the EU where the country or entity to which such data is transferred ensures an adequate level of protection for personal data. This requirement is enshrined in Article 25(1) of Directive 95/46/EC (in respect of matters falling within the Directive's scope) and is also reflected in Article 5 of the Agreement. In assessing the adequacy of the level of protection for personal data, the presence of an effective independent mechanism for supervision of data processing is clearly an important consideration. While the concept of "adequate" in Article 25(6) of Directive 95/46/EC has been interpreted as

[13] See e.g. Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, p. 4.
[14] Agreement, Article 16(3)-(4).
[15] See e.g. Judgment in *Commission v. Germany*, C-518/07, EU:C:2010:125; Judgment in *Commission v. Austria*, C-614/10, EU:C:2012:631; Judgment in *Commission v. Hungary*, C-288/12, ECLI:EU:C:2014:237.
[16] Judgment in *Schrems*, C-362/14, EU:C:2015:650, paragraphs 44-45.

requiring a third country to ensure "a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union",[17] this Court has recognised that the means to which a third country has recourse in this connection "may differ from those employed within the European Union…".[18]

In the case of the Agreement, Article 10 provides for two mechanisms for oversight. The Note of the Mission of Canada to the European Union dated 25th June 2014 confirms that the Privacy Commissioner of Canada is the "independent public authority" and that the Recourse Directorate, Corporate Affairs Branch of the Canada Border Services Agency is the "authority created by administrative means" referred in Article 10 of the Agreement. According to the Note, the Privacy Commissioner has oversight over the data protection rules in the Privacy Act and will be the primary recourse authority for individuals present in Canada while the Recourse Directorate of the CBSA will be the primary recourse authority for individuals not present in Canada. While the Privacy Commissioner may be considered as satisfying the requirements of the Court's case-law, it may be questioned whether the Recourse Directorate satisfies the requirement of "independence" in that case-law. In particular, although the Recourse Directorate exercises its functions without interference from other functional areas of the Canada Border Services Agency and carries out its reviews and arrives at its decisions in an impartial and independent manner, it is structurally integrated within the Canada Border Services Agency.[19] As the Commission has explained in its Observations, while recourse to the Privacy Commissioner for the purposes of requesting access to one's data (for example, for the purpose of correcting the data) is limited to nationals, permanent residents and persons present in Canada, and the additional administrative mechanism provided by the Recourse Directorate was consequently necessary, *any* individual can submit a complaint to the Privacy Commissioner if the individual considers that a federal public institution (such as the Canadian Competent Authority in this case) has engaged in illegal data processing.[20] In this way, compliance with the rules governing the processing of PNR data is subject to control by an independent authority.

In Ireland's submission, notwithstanding the different institutional means chosen by Canada for the purposes of supervising PNR data processing, the oversight mechanisms established under Article 10 of the Agreement, understood as a whole, provide an adequate level of protection for personal data transferred from the EU to

[17] Judgment in *Schrems*, C-362/14, EU:C:2015:650, paragraph 73.
[18] Judgment in *Schrems*, C-362/14, EU:C:2015:650, paragraph 74.
[19] See the judgment in *Commission v. Austria*, EU:C:2012:631.
[20] Written Observations of the Commission, paragraphs 105-106.

Canada and are, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union. In this regard, it is relevant to bear in mind the specific characteristics of the data processing involved under the Agreement which relate to a relatively discrete category of data and solely for the purposes of preventing, detecting, investigating and prosecuting terrorism or serious transnational crime.

7. To what extent do Articles 6, 18 and 19 of the draft agreement, respectively permitting sharing of PNR data and analytical information with European authorities and disclosure of PNR data to other government authorities in Canada and to other third-country authorities, fulfil the requirements of the case-law referred to in point II.4?
In particular, as regards the disclosure of PNR data to authorities of other third countries, in so far as compliance with the rule laid down in Article 19(1)(e) of the draft agreement is restricted to a Canadian authority and the third countries to which the PNR data may be disclosed are not specified in advance, can that rule be regarded as effective?

In Ireland's view, Articles 6, 18 and 19 of the Agreement lay down clear and precise rules regulating the onward transfer of PNR data to government authorities within the EU, Canada and third countries and impose a series of effective safeguards to protect personal data in this context. This being so, Ireland submits that the provisions fulfil the requirements laid down by this Court in its judgments in *Digital Rights Ireland* and *Schrems*.

With reference to Article 6 of the Agreement, it is important to emphasize that this provision permits the sharing of PNR data and analytical information only with European Union Member States or agencies (specifically, Europol and Eurojust) and in accordance with relevant information-sharing or law enforcement agreements. While Articles 18 and 19 of the Agreement relate to disclosure of PNR data to government authorities in Canada or in third countries respectively, both provisions are framed in the negative and permit such disclosure only if a series of strict cumulative conditions are met.

Under Article 18(1) of the Agreement, the Canadian Competent Authority cannot disclose PNR data to other government authorities in Canada unless six conditions are met. Disclosure is only permissible to government authorities whose functions are directly related to the scope of Article 3 and in circumstances where it is necessary for the purposes stated in Article 3 (that is, the prevention, detection, investigation or prosecution of terrorist offences or serious transnational crime): Article 18(1)(a) and

(c). It must be on a case-by-case basis (Article 18(1)(b)) and involve disclosure of the minimum amount of PNR data necessary (Article 18(1)(d)). The receiving government authority must afford equivalent protection to the safeguards enshrined in the Agreement (Article 18(1)(e)) and cannot, without authorisation from the Canadian Competent Authority, engage in any onward transfer of the data (Article 18(1)(f)). These conditions therefore strictly regulate the onward transfer of PNR data by the Canadian Competent Authority to other government authorities in Canada and ensure that PNR data is used only for purposes, and under conditions, consistent with those enshrined in the Agreement.

Similarly, under Article 19(1) of the Agreement, disclosure of PNR data by the Canadian Competent Authority to government authorities in third countries is subject to strict conditions. In relation to Article 19(1)(e) of the Agreement specifically, this provides that PNR data cannot be disclosed unless the Canadian Competent Authority is satisfied that: (i) the foreign authority receiving the PNR data applies standards to protect the PNR data that are equivalent to those set out in the Agreement, in accordance with agreements and arrangements that incorporate those standards; or (ii) the foreign authority applies standards to protect the PNR data that it has agreed with the European Union. This provision must be understood in the context of the practical issues raised by the control of onward transfers of data outside the EU. Once PNR data is transferred to the Canadian Competent Authority, it is that authority which, in practical terms, must oversee any onward transfer of PNR data. It would not be feasible, in practice or in principle, for EU or EU Member State authorities to oversee this process. All the EU can do, within the context of the Agreement, is to ensure that the Canadian Competent Authority permits such onward transfer of PNR data under strict conditions which are binding on Canada as a matter of international law. Article 19(1)(e)(ii) envisages disclosure to a foreign authority which is already bound by the standards and safeguards laid down in an agreement with the EU. Under Article 19(1)(e)(i), the Canadian Competent Authority must be satisfied that the foreign authority receiving the PNR data "applies standards to protect the PNR data that are equivalent to those set out in the Agreement, in accordance with agreements and arrangements that incorporate those standards". While Article 19(1)(e)(i) does not require *a priori* EU approval of those standards and does not specify the third countries to which the provision may apply (which are likely to change over time), it is confined to circumstances where Canada has incorporated those standards in agreements or arrangements. In addition, Article 19(2) of the Agreement provides an important safeguard by imposing a notification requirement on the Canadian Competent Authority in the case of any disclosure of PNR data of a citizen of an EU Member State. In view of the importance of facilitating international cooperation in the fight against terrorism and serious transnational crime, and the very real practical

challenges in regulating onward transfers by third countries, Ireland submits that the rule laid down in Article 19(1)(e) of the Agreement can be regarded as effective.

8. Article 14(2) of the draft agreement provides that 'any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek effective judicial redress in accordance with Canadian law by way of judicial review, or such other remedy ...'.
As regards the latter possibility, can it be said that judicial scrutiny is actually guaranteed?

In Ireland's view, Article 14(2) of the Agreement must be interpreted as meaning that Canada *shall* ensure that an individual – who is of the view that their rights have been infringed by a decision or action in relation to their PNR data – has the option *either* to seek effective judicial redress in accordance with Canadian law by way of judicial review *or* "such other remedy which may include compensation". The remedies are framed, and must be interpreted, as alternatives. In this way, affected individuals are guaranteed effective judicial redress and scrutiny. However, the guarantee of effective judicial protection does not exclude the availability of alternative non-judicial remedies, particularly remedies which may be more accessible, practical and effective for affected individuals. By way of analogy, within the EU's data protection regime, while Article 22 of Directive 95/46/EC requires Member States to provide for "the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question", this is expressed as being "without prejudice to any administrative remedy for which provision may be made" *inter alia* before the national supervisory authority. The availability of such an alternative remedy does not detract from the guarantee of judicial protection.

9. To what extent does the draft agreement include rules aimed at facilitating cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions (Article 82(1)(d) TFEU)?

In Ireland's view, by putting in place a common framework governing the transfer and processing of Passenger Name Record data between the European Union and Canada, the Agreement as a whole facilitates cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions within the meaning of Article 82(1)(d) TFEU. More specifically, Article 6 of the Agreement, which deals with police and judicial cooperation, contains rules which facilitate cooperation among Member States in the context of the fight against terrorism and serious transnational crime.

Article 6(1) requires Canada to share, as soon as practicable, "relevant and appropriate analytical information containing PNR data obtained under this Agreement with Europol, Eurojust, within the scope of their respective mandates, or the police or a judicial authority of a Member States of the European Union". Article 6(2) requires Canada, at the request of those same authorities, to share PNR data or analytical information containing PNR data obtained under the Agreement "in specific cases to prevent, detect, investigate or prosecute within the European Union a terrorist offence or serious transnational crime". Article 19(2) of the Agreement, concerning disclosure outside Canada, and Article 23, on reciprocity, are also relevant in this regard.

In Ireland's view, the concept of rules facilitating cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters or the enforcement of decisions, within Article 82(1)(d) TFEU, is not confined to rules facilitating cooperation among Member State authorities *inter se*. This concept has an important external dimension, particularly in the context of the fight against global challenges such as terrorism and serious transnational crime which, by their very nature, frequently require international cooperation between the EU and third countries. This Court has long recognized that, even where the Treaties do not expressly confer competence on the Union to conclude international agreements in a particular field, the Union may have implied power to act in certain circumstances.[21] This is now reflected in Article 216(1) TFEU which provides that the Union may conclude "with one or more third countries or international organisations where the Treaties so provide or where the conclusion of an agreement is necessary in order to achieve, within the framework of the Union's policies, one of the objectives referred to in the Treaties, or is provided for in a legally binding Union act or is likely to affect common rules or alter their scope". It is on the basis of such an implied power that the Union has concluded a series of international agreements in fields which touch upon judicial or police cooperation in criminal matters.[22] As Advocate

[21] Judgment in *Commission v. Council*, Case 22/70, EU:C:1971:32; Opinion 1/03, *Lugano Convention*, EU:C:2006:81.

[22] Council Decision 2010/482/EU of 26 July 2010 on the conclusion of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; Council Decision 2010/616/EU of 7 October 2010 on the conclusion of the Agreement between the European Union and Japan on mutual legal assistance in criminal matters; 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; Council Decision 2012/472/EU of 26 April 2012 on the conclusion of the Agreement between the

General Bot has observed in his Opinion in Case C-130/10, "the external dimension that may attach to the European Union's actions under its policy of creating an AFSJ should not be disregarded".[23]

10. To what extent is Article 16 TFEU capable of constituting a legal basis for the adoption of rules which appear to concern the collection and processing of personal data *by individuals and by the authority of a third country* and not by EU institutions, bodies, offices and agencies or by the Member States when carrying out activities which fall within the scope of EU law?

In Ireland's view, Article 16 TFEU is not capable of constituting a legal basis for the adoption of rules concerning the collection and processing of personal data by individuals and by the authority of a third country, as opposed to by EU institutions, bodies, offices and agencies or by the Member States when carrying out activities which fall within the scope of EU law. The rules adopted under Article 16 TFEU – which also includes reference to rules relating to the free movement of personal data – may of course have an external dimension and, in particular, may regulate the transfer of personal data to third countries. However, for the reasons set out in its observations, Ireland submits that Article 16 TFEU is not an appropriate legal basis for the Agreement at issue in these proceedings, which has its aim ensuring public security and safety and which thus properly falls within the scope of Title V of the Treaty on the Functioning of the European Union.

Dated the 3rd day of March 2016

Signed: Gemma Hodge
Agent for Ireland on behalf of Eileen Creedon, Chief State Solicitor

Signed: Tony Joyce
Agent for Ireland on behalf of Eileen Creedon, Chief State Solicitor.

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.

[23] Opinion in *Parliament v. Council*, C-130/10, EU:C:2012:50, paragraph 10.