The European Court of Justice on the EU-Canada Passenger Name Record Agreement

ECJ, 26 July 2017, Opinion 1/15

Arianna Vedaschi*

INTRODUCTION

In a world constantly struggling against the continuing threat of international terrorism since the events of 2001, which has grown even stronger in recent years, the rights to privacy and data protection are frequently curtailed by counter-terrorism policies in an attempt to guarantee security. Surveillance measures entailing an indiscriminate collection and retention of data, which are then accessed and analysed by intelligence agencies, are examples of this.[1] These mechanisms are ensconced in both national and EU law (indeed, the latter often influences the former). Among the EU's tools, not only could one point to certain directives that explicitly call upon Member States to collect and retain a wide range of data for crime prevention purposes,[2] but also to several international agreements signed by the EU and third countries, on which this case comment will focus. In this context, the information at stake is frequently collected haphazardly and without distinction, and does not necessarily pertain to terrorist suspects.

*Full Professor of Comparative Public Law at Bocconi University of Milan.

[1] For a recent analysis, D. Cole et al. (eds.), *Surveillance, Privacy and Transatlantic Relations* (Hart Publishing 2017) and M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing 2017) p. 107.

[2] In reference to both Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006, L 105/54 (Data Retention Directive, held invalid by the Court) and the recent Directive (EU) 2016/681 of the 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, OJ 2016, L 119/132.

European Constitutional Law Review, 14: 410–429

doi:10.1017/S1574019618000202

Indeed, not all EU institutions are firmly committed to a securitarian attitude.[3] The Council and the Commission appear to follow this trend, commonly allowing security to prevail over rights. In this respect, it is enough to consider their approach to asset freezing: they implemented UN resolutions imposing financial sanctions on suspect terrorists, regardless of their rights to property and, above all, a fair trial.[4] The European Parliament, instead, often takes privacy and data protection more seriously. For example, in the case that is going to be analysed, it asked the European Court of Justice to assess the compatibility of antiterrorism measures with fundamental rights. Over the last few years, the Court of Justice has played a key role in striking a balance between the rights to privacy and data protection on the one hand, and public security, on the other. Examples of the Court's case law range from the *Digital Rights Ireland* decision[5] of 2014, in which the Data Retention Directive was quashed[6] due to human rights concerns, to the *Schrems* judgment[7] that, in 2015, invalidated the Commission adequacy decision on which the *Safe Harbour* (i.e. the agreement regulating the exchange of personal data between the EU and the US) was grounded. Principles affirmed in *Digital Rights* were reiterated in *Tele2 Sverige AB*,[8] again dealing with data retention (this time, envisaged by national law) and human rights, after a request for preliminary ruling by British and Swedish courts.

Opinion 1/15 was issued by the Court of Justice at the request of the Parliament, pursuant to Article 218(11) TFEU. The Parliament asked the Court to rule on the compatibility with EU law of the draft Agreement between the EU and Canada on the exchange of Passenger Name Record data. In July 2017, the

[3] On the EU's attitude towards security, S. Carrera and V. Mitsilegas (eds.), *Effectiveness, Rule of Law and Rights in Countering Terrorism and Crime* (CEPS 2017); for a comparative overview of security measures enacted by Member States after 9/11, A. Vedaschi, *À la guerre comme à la guerre? La disciplina della guerra nel diritto costituzionale comparato* (Giappichelli 2007) p. 526.

[4] This attitude was opposed by the ECJ in the so-called *Kadi* saga. *See further* C. Gearty, 'In Praise of Awkwardness: Kadi in the CJEU', 10 *EuConst* (2014) p. 15.

[5] ECJ 8 April 2014, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. See* A. Vedaschi and V. Lubello, 'Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective', 20 *Tilburg Law Review* (2015) p. 14; O. Linskey, 'The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: *Digital Rights Ireland*', 51 *Common Market Law Review* (2014) p. 1789.

[6] Directive 2006/24/EC, *supra* n. 2.

[7] ECJ 6 October 2015, Case C-362/14, *Maximillian Schrems v Data Protection Commissioner. See* L. Azoulai and M. Van der Sluis, 'Institutionalizing personal data protection in times of global institutional distrust', 53 *Common Market Law Review* (2016) p. 1343 and T. Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter', 12 *EuConst* (2016) p. 318.

[8] ECJ 21 December 2016, Case C-203/15, *Tele2 Sverige AB* v *Post- och telestyrelsen* and *Secretary of State for the Home Department* v *Tom Watson and Others*.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press

Court found that Agreement incompatible with fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. The Court's Opinion should be regarded as a noteworthy effort to weigh up competing interests.

After an overview of the factual and legal background, this case comment retraces the main steps of the Court of Justice's reasoning. Specifically, this analysis addresses three critical areas arising from the Opinion: (i) its practical impact, meaning the (already expressed or foreseeable) reactions of other EU institutions, and subsequent changes in EU law concerned with privacy; (ii) its standing within the abovementioned established case law of the Court; and (iii) whether and how the relationship between rights and security will be affected by mass surveillance, which – under strict conditions – is allowed in the age of terrorism.

Passenger Name Record Agreements in EU law

Passenger Name Record data include information such as names, travel dates, itineraries, seats, baggage, contact details, means of payment and many other facts related to the life and habits of travellers. The transfer of data collected by airline carriers to the authorities of third countries towards which flights are headed[9] has been regulated over time by several agreements signed between the EU and non-EU countries to prevent and counter international terrorism. Data can be collected, alternatively, through the 'push' or 'pull' methods. The latter simply means that the authority vested with the power to collect it can directly access the data; the former method implies a data request to an air carrier. Pursuant to Article 25 of Directive 95/46/EC,[10] in order to allow the exchange of Passenger Name Record data between the EU and a third country, the third country must ensure an 'adequate level of protection', certified by the European Commission through a so-called adequacy decision based on the existence of appropriate guarantees in the third country's domestic law or in its international commitments. According to the Court of Justice, an 'adequate level of protection' means that protection must be 'essentially equivalent'[11] to that guaranteed by the EU.

[9] The equivalent of the Passenger Name Record regime with regard to the transfer of financial data is the Terrorist Finance Tracking Programme. This Agreement between the EU and the US came into force in 2010 and concerns the transfer and processing of data for purposes of identifying, tracking and pursuing terrorists and their networks. *See* C.C. Murphy, *EU Counter-Terrorism Law* (Hart Publishing 2015) p. 151.

[10] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31.

[11] Schrems, supra n. 7. See R.A. Epstein, 'The ECJ's Fatal Imbalance: Its Cavalier Treatment of National Security Issues Poses Serious Risk to Public Safety and Sounds Commercial Practices', 12 *EuConst* (2016) p. 330 at p. 334, discussing the Court of Justice's equation between 'adequate protection' and 'essential equivalence'.

The need to deal with Passenger Name Record exchange arose for the first time in 2001, when US legislation[12] obliged airline carriers travelling to the US to transfer passengers' data to US Customs and Border Control.[13] Therefore, the European Commission needed to reach an agreement with US authorities on the transfer of Passenger Name Record data. This agreement, signed on 28 May 2004,[14] had several controversial aspects. First of all, it provided US officials with direct access to data (pull system), without any active participation in the transfer of data by airline carriers. In addition, the reasons justifying data collection were vague and the retention period was long (three and a half years, which can be extended in case of investigation).[15] For these reasons, the EU-US Passenger Name Record Agreement was challenged before the Court of Justice by the Parliament, which called for the annulment of both the Council decision on the conclusion of the Agreement and the Commission adequacy decision.[16] The Court annulled both, arguing that an incorrect legal basis had been invoked.[17] Specifically, the EU institutions had acted within the first pillar, i.e. the internal market, while the Court held that they should have acted within the third pillar, i.e. cooperation in the fields of justice and home affairs, since the fight against terrorism and serious crime was the main purpose of

[12] US Aviation and Transportation Security Act 2001, Pub L 107-71. It is also worth noting that the US restrictive approach towards privacy depends on the fact that, in such areas, privacy is traditionally considered to be a relative right which can be limited by many competing interests. On the US attitude towards privacy and data protection, M.W. Price, 'Rethinking Privacy: Fourth Amendment Papers and the "Third-Party" Doctrine', 8 *Journal of National Security Law and Policy* (2016) p. 247.

[13] The main federal law enforcement agency, whose tasks include the protection of borders from entry by terrorists and criminals in general.

[14] Council Decision 2004/496/CE of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004, L 183/84.

[15] On the controversial aspects of this system, *see* B. Siemen, 'The EU-US Agreement on Passenger Name Records and EC Law: Data Protection Competences and Human Rights Issues in International Agreement of the Community', 47 *German Yearbook of International Law* (2005) p. 629. More widely on previous Passenger Name Record agreements, V. Papakostantinou and P. De Hert, 'PNR Agreement and Transatlantic Antiterrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic', 46 *Common Market Law Review* (2009) p. 885.

[16] According to former Art. 230 of the Treaty on the European Community (current Art. 236 TFEU).

[17] ECJ 30 May 2006, Joined Cases C-317/04 and C-318/04, *European Parliament v Council of the European Union and Commission of the European Community*. For an analysis of this decision, see G. Gilmore and J. Rijpma, 'Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission, Judgment of the Grand Chamber of 30 May 2006 [2006] ECR-I04721', 44 *Common Market Law Review* (2007) p. 1081.

the agreement. As a consequence, the EU institutions were urged to enter into a new agreement.

On 23 July 2007, the Council approved a new Passenger Name Record Agreement,[18] which incidentally raised even more concerns in terms of fundamental rights than the first version. In particular, a wider variety of data could be collected, encompassing also some sensitive data (although a filtering mechanism was provided) and the retention period was extended (up to seven years). Additionally, there were no 'robust legal mechanisms'[19] enabling people to challenge the potential misuse of their data. The shift from the 'pull' to the 'push' system in data sharing marked the only improvement in terms of rights protection. Once again, the Parliament considered guarantees for passengers' rights to be insufficient and passed a resolution asking for the renegotiation of the Agreement.[20]

The third and current Passenger Name Record Agreement between the EU and the US has been in force since 1 July 2012 and has not been challenged before the Court.[21] It secures several important guarantees (e.g. by delimiting the purpose and duration of data retention), but still leaves wide discretion to US authorities in determining exceptions to the retention period and to the anonymisation of data.[22]

Canada enacted rules on Passenger Name Record similar to those legislated by the US[23] and in 2005 the EU entered into an Agreement with that country too.[24]

[18] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS). This Agreement had been preceded by an interim version, in which many rights-related concerns could be found. *See* the Agreement between the European Union and the United States on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security [2006] OJ 2007, L 204/16,

[19] Letter from Peter Hustinx, European Data Protection Supervisor, to Wolfgang Schäuble, Minister for the Interior (27 June 2007), <www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf>, visited 19 March 2018.

[20] European Parliament Legislative Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada P7 TA (2010)0144.

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

[22] For an overview of the contents and critical aspects of this agreement, *see* A. Vedaschi and G. Marino Noberasco, 'From DRD to PNR: Looking for a New Balance Between Privacy and Security', in Cole, *supra* n. 1, p. 67.

[23] Anti-Terrorism Act, SC 2001, C 41.

[24] 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, OJ 2006, L 82/14.

That deal's major flaws are similar to those identified in the above-mentioned EU-US Agreements. Although the EU-Canada Agreement provided for a 'push' system and envisaged a difference in retention times depending on whether the passengers were under investigation, it included a few controversial provisions on data re-personalisation and complex administrative procedures for filing complaints.[25]

When the Agreement with Canada expired in 2009, negotiations once again got underway and a new Agreement was signed on 25 June 2014.[26] Parliament, worried about the detrimental effect certain provisions could potentially have on human rights, triggered the Article 218(11) TFEU procedure, which entitles it to seek the opinion of the Court of Justice on the compatibility of an international agreement with the EU Treaties before its approval and definitive entry into force.[27]

The Opinion of Advocate General Mengozzi

On 8 September 2016, Advocate General Paolo Mengozzi held, in his Opinion to the Court,[28] that several provisions of the Passenger Name Record Agreement were patently contrary to Articles 7 (the right to privacy), 8 (the right to data protection) and 52 (the principle of proportionality) of the Charter.[29]

As a first step, in considering the existence of any interference with the rights to privacy and data protection, the Advocate General maintained that a serious interference did exist[30] because the intrinsic characteristics of the collected data revealed a great deal about the lives and habits of passengers. Consequently, the right to privacy under Article 7 and the 'closely connected but nonetheless distinct'[31] right to data protection under Article 8 of the Charter were impaired.

The second step of Mengozzi's Opinion focused on the justifiability of such an interference, as assessed under the scheme set forth in Article 52 of the Charter. According to this provision, three aspects must be taken into account: first, whether the interference is provided for by law and respects the essence of the

[25] For an overview of this regime, *see* P. Hobbing, 'Tracing Terrorists: The EU-Canada Agreement in PNR Matters', Special Report, *Center for European Policy Studies,* 17 November 2008, available at <aei.pitt.edu/11745/1/1704.pdf>, visited 19 March 2018.

[26] Council of the European Union, Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 2013/0250 (NLE).

[27] European Parliament Resolution of 25 November 2014 on seeking an opinion from the ECJ on the compatibility with the Treaties of the Agreement between Canada and the EU on the transfer and processing of Passenger Name Record data P8_TA (2014) 0058.

[28] Case 1/15, Opinion of AG Mengozzi, 8 September 2016.

[29] On the procedural side, the AG remarked that Art. 16(2) TFEU can be invoked as an appropriate legal basis for such an agreement, together with Art. 87(2)(a) TFEU, read in conjunction with Art. 218(6)(a)(v).

[30] Opinion of AG Mengozzi, para. 180.

[31] *Ibid.*, para. 170.

right; second, whether it pursues a legitimate aim; and third, whether it complies with the principle of proportionality.[32] As to the first criterion, from a formal point of view, the Advocate General considered the interference provided for by law: pursuant to the EU Treaties, once all phases for their approval have been concluded, international agreements become part of EU law.[33] From a substantive perspective, according to Advocate General Mengozzi, the Agreement is clear, accessible and foreseeable enough to meet the standards in terms of 'quality of the law' as required by the Court of Strasbourg's case law.[34] Last but not least, the essence of the right is not impaired, since a mechanism of gradual depersonalisation of data does not allow specific conclusions to be drawn on the private lives of the persons concerned.[35]

Given the correspondence between the proclaimed goal of the Agreement, i.e. combating terrorism and other serious crime, and the 'general interest' prescribed by Article 52 of the Charter, the Advocate General examined the proportionality of the means employed, stressing the necessity of strict scrutiny, also in light of the *Digital Rights* and *Schrems* judgments.[36] From this perspective, the Advocate General noted that, even if the means had been suitable for pursuit of the aim,[37] they were not strictly necessary. On the one hand, according to Mengozzi's Opinion, sensitive data should be excluded; on the other, an exhaustive list of 'serious offences' should be drawn up. Moreover, the Advocate General pointed out the very long retention period, which could not be justified for any objective reason:[38] pursuant to the Agreement, all data must be retained for five years from the date of collection, albeit 'masked' after 30 days. However, under specific circumstances – such as investigative necessity – they could be unmasked. Thus, data are simply pseudonymised, rather than anonymised (the difference between the two being in fact that anonymisation is irreversible, whilst pseudonymisation is not). Pseudonymised data do not cease to fit the category of 'personal data'; this means that data protection guarantees still apply (which would be different if the data had been anonymised).[39] Additionally, the Advocate General criticised the

[32] On which, *see* S. Peers and S. Prechal, 'Article 52. Scope and Interpretation of Rights and Principles', in S. Peers et al. (eds.), *The EU Charter of Fundamental Rights. A Commentary* (Hart Publishing 2014) p. 1455.

[33] Opinion of AG Mengozzi, para. 192.

[34] *Ibid.*, para. 193.

[35] *Ibid.*, para. 186.

[36] *Ibid.*, paras. 199-204.

[37] *Ibid.*, paras. 205-206.

[38] *Ibid.*, para. 279.

[39] On the use of anonymisation, *see* C.C. Cocq, 'Encryption and Anonymisation Online: Challenges for Law Enforcement Authorities Within the EU', in T. Bräutigam and S. Miettinen (eds.), *Data Protection, Privacy and European Regulation in the Digital Age* (Unigrafia 2016) p. 178.

indiscriminate application of the measures, irrespective of any suspicion of involvement in terrorist activity.[40] Furthermore, these flaws were combined with the vaguely defined Canadian authority tasked with processing the data, a lack of strict rules on access to data and the uncertain reference to judicial remedies.

Concluding his Opinion, Advocate General Mengozzi warned EU institutions against the adoption of the Agreement in its current version. Although admitting that there were ways to bring Passenger Name Record data transfer into compliance with human rights protection,[41] he stated that this was not the case with the 2014 EU-Canada Agreement.

The Court of Justice's Opinion: main points

The Court of Justice delivered its Opinion on 26 July 2017,[42] adhering to the Advocate General's stance and arguing that the Agreement could not be adopted in its current form. Although EU institutions could even decide not to adopt any agreement at all, in October 2017 the Commission issued a recommendation for a Council decision on re-opening negotiations in compliance with the Court's Opinion.[43] Therefore, it is likely that a new agreement will be signed to avert – among other things – the impairment of EU-Canada relations.

In its ruling, the Court addressed both parts of Parliament's request, i.e. the appropriate legal basis for the Council decision on the conclusion of the Agreement and the compatibility of the text with Articles 7 and 8, read in light of Article 52 of the Charter.

As to the first question, the Council decision was based on Articles 82(1)(d) and 87(1)-(2)(a) TFEU, concerning measures that facilitate judicial cooperation among Member States in relation to criminal matters and measures on the collection of information aimed at police cooperation, respectively. The Parliament claimed that the correct legal basis was instead Article 16 TFEU,[44] which ensures the protection of personal data and empowers the Council and the Parliament to enact measures regulating their processing. According to the Court of Justice, the Agreement should have been based on Articles 16 and 87(2)(a) jointly,[45] but not on Article 82(1)(d). In particular, the Court argued that there were no provisions envisaging a facilitation

[40] *Ibid.*, para. 222.

[41] *Ibid.*, para. 285. Specifically, the masking and progressive depersonalisation of data would guarantee respect for the concerned rights.

[42] ECJ 26 July 2017, Opinion 1/15. For a short comment, C. Graziani, 'PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali', *DPCE online* (2017) p. 959.

[43] COM(2017) 605 final.

[44] ECJ 26 July 2017, Opinion 1/15, para. 97.

[45] *Ibid.*, para. 98.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press

of judicial cooperation and that the Canadian authority in charge of the use of Passenger Name Record data was not a judicial authority, nor equivalent to one. In order to reach its conclusion, the Court underlined that the Agreement has a twofold aim: the transfer of Passenger Name Record data must both serve the interest of public security and respect the rights to privacy and data protection. The Court noted that such objectives lie within the scope of both Articles 16 and 87(2)(a) TFEU and reiterated that the transfer of Passenger Name Record data to third countries cannot take place unless an 'adequate level of protection' is demonstrated,[46] i.e. the level of protection must be 'essentially equivalent'[47] to that guaranteed by the EU.

The Court of Justice went on to evaluate the compatibility of the Agreement with the standards set by the TFEU and the Charter. And the Court remarked that, in the case at hand, only Article 8 of the Charter should be regarded as a parameter for data protection, without separately considering Article 16 TFEU, the former being more specific than the latter.

First of all, the Court of Justice found an interference with the rights concerned; Passenger Name Record data reveal information that allows identification of the personal data of specific individuals, which must then be processed within the meaning of Article 8 of the Charter.[48] In order to assess whether such an interference is justified, the Court examined the basis for its limitation, finding it[49] to be legitimate, laid down by law and pursuing an objective of general interest (public security). Moreover, such interference did not affect the essence of the rights concerned.

However, when extensively addressing the necessity of the interference, the Court of Justice considered several EU law parameters violated by the current text of the Agreement.

First, the Court argued that it was not clear which types of Passenger Name Record data were covered by the Agreement.[50] For example, use of the word 'etc.' was criticised,[51] as well as the expression 'all available contact information'.[52] In addition, the transfer may include sensitive data, which were then transferred and

[46] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L 281/31.

[47] *Maximilian Schrems* v *Data Protection Commissioner*, *supra* n. 7, para. 73.

[48] Opinion 1/15, para. 126.

[49] I.e. the agreement itself, and not the consent. According to Art. 8 of Charter, a limitation can be based, alternatively, on explicit consent of data subjects or on another legitimate basis laid down by law.

[50] Opinion 1/15, para. 163.

[51] *Ibid.*, para. 157.

[52] *Ibid.*, para. 158.

processed with no solid justification. Remarkably, prevention of terrorism was not deemed to be justification by the Court.[53]

Second, the Court of Justice addressed automatic processing. According to the Agreement,[54] data are collected and automatically analysed, and cross-checked against databases containing information on suspect terrorists; if any profiles match, the analysis is repeated in a non-automated manner in order to decide whether it is necessary to take individual measures against targeted passengers. The Court welcomed the fact that automatic processing has to be followed by a re-examination through non-automated means.[55] It did, however, specify that the databases against which data are cross-checked must be 'reliable, up to date and limited to databases used by Canada in relation to the fight against terrorism and serious transnational crime'.[56]

Third, the Court of Justice found some of the purposes for processing Passenger Name Record data to be unclear, not well enough defined. Although the definitions of 'terrorist offence' and 'serious transnational crime' were well specified,[57] the Agreement stated that Passenger Name Record data could also be processed for 'other purposes' which were not specified in detail.[58]

The fourth and fifth points analysed by the Court, i.e. the competent Canadian authority charged with processing the data and the passengers affected by measures contained in the Agreement, were deemed to comply with EU law standards since they were defined with sufficient clarity and precision.[59]

Sixth, there were no clear and precise rules on the retention of data. The Court of Justice recalled that there must be a connection, based on objective criteria, between the retention of personal data and the aim pursued by the Agreement.[60] In addition, data use must be regulated by substantive and procedural conditions.[61] According to the Agreement, data could be retained and used before the arrival of passengers, during their stay in Canada, upon and even after their departure.[62] The Court of Justice warned that post-departure data retention is particularly tricky. Since such data have in fact already been checked and verified, continued retention should not be necessary, unless there are objective

[53] *Ibid.*, para. 165.
[54] Art. 15 of the Agreement.
[55] Opinion 1/15, para. 173.
[56] *Ibid.*, para. 172.
[57] *See* Art. 3(2)-(3) of the Agreement.
[58] Opinion 1/15, para. 181.
[59] *Ibid.*, paras. 185 and 189.
[60] *Ibid.*, paras. 190-191.
[61] Citing the *Schrems* and *Tele2* decisions.
[62] As already stated, the retention period is five years. Notably, the Court deemed this length admissible (para. 209 of the Opinion).

reasons that require doing so.[63] On the contrary, as to retention and use before passengers' arrival and during their stay in Canada, the Court acknowledged the existence of a connection with the pursued objective. Nonetheless, rules about retention and use were found to exceed what is strictly necessary,[64] due to the lack of a review procedure (carried out by a judicial or an independent administrative body) on use of data pertaining to passengers staying in Canada.

Lastly, the Court of Justice analysed provisions concerning disclosure. The Agreement allowed the disclosure of data to Canadian and third-country authorities, as well as, under certain circumstances, to individuals. In all these cases, the concerned measures did not comply with the strict necessity test. While disclosure of data to Canadian authorities should respect rules governing the use of data, such rules are nonetheless not well-defined.[65] Additionally, the Court noted that, in order to avoid disclosure to the authorities of third countries masking a circumvention of guarantees enshrined in EU law, an agreement between the EU and the third country or a Commission adequacy decision should certify an equivalent level of protection. The EU-Canada Passenger Name Record Agreement did not require this; therefore, disclosure was not limited to what is strictly necessary.[66] As to disclosure to individuals, which is allowed when the 'legitimate interests of the individual [are] concerned', the Court found a major flaw; the Agreement did not specify legal requirements and limitations, concerned interests, envisaged purposes or judicial or administrative oversight.[67]

After assessing the necessity and proportionality of the interference, the Court of Justice examined two further important aspects of the Agreement: passengers' guarantees and oversight mechanisms. As to the first issue, the Court condemned the lack of a system of notification. In other words, passengers should be made individually aware of the use and processing of their data.[68] As to the second, the Agreement stated that data protection safeguards would be subject to the oversight of an 'independent public authority' or an 'authority created by administrative means that exercised its functions in an impartial manner and that has proven a record of autonomy'. According to the Court, the use of this alternative wording implied that oversight, or at least part of it, could hypothetically be carried out by a body that is not fully independent.[69] Hence, the Agreement did not ensure complete independence during the oversight process.

[63] Opinion 1/15, paras. 204-207.
[64] *Ibid.*, para. 203.
[65] *Ibid.*, para. 212.
[66] *Ibid.*, para. 214.
[67] *Ibid.*, paras. 216-217.
[68] *Ibid.*, para. 225.
[69] *Ibid.*, para. 231.

Reading Opinion 1/15

In order to analyse this Opinion, it is worth focusing on two crucial aspects. Firstly, the Court of Justice allowed mass surveillance as a matter of principle, but only if it respected certain detailed and strict requirements that were perhaps not easy to implement. Therefore, there was a sort of discrepancy between what was theoretically acceptable and what was practically achievable – or, at least, had been achieved until that moment. Secondly, the Court caused a sort of 'revolution' in the EU institutional allocation of powers, insofar as it addressed the wording and technical mechanisms of the Agreement in such a manner that it seemed to take over the role of a legislative body, concretely drafting a normative text.

The following analysis will concentrate on these two points, highlighting the importance of the Opinion and its remarkably innovative features. As to guidelines emerging from this decision, the Court clarified, once again and more specifically than in other decisions, that the transfer, retention and use of Passenger Name Record data could be deemed compatible with guarantees enshrined in EU law as long as they respected certain specific conditions.

First, the categories of Passenger Name Record data covered by the Agreement should be clearly and precisely indicated and this had not been done in some of the cases listed in an ad hoc Annex. From this perspective, the Court even criticised the wording of some of its headings, engaging in a particularly careful and detailed analysis.[70] In this passage, strict scrutiny is prescribed. In other words, in a (successful) attempt to secure the highest level of protection for individuals, the Court did not merely concern itself with appearances; it determined that the Agreement's drafting was unacceptably vague, even if the list of Passenger Name Record data provided by its Annex contained a delimitative clause,[71] hence making it exhaustive.[72] In this way, the Court of Justice built upon previous decisions in which it had abstractly affirmed the need for an exhaustive list.[73] This time, though, the Court scrutinised the merits of such a list, thus demonstrating the substantive nature of its review. Moreover, the strong claim of excluding sensitive data was to be expected, since other recent EU legislation contained the same prohibition. For example, Directive 2016/681,[74] dealing with Passenger

[70] An emblematic example is the criticism of the term 'etc.' in Heading 5. *See* Opinion 1/15, para. 157.

[71] Art. 4(3) of the Agreement, stating that all data that are not listed must be deleted.

[72] Opinion 1/15, para. 162.

[73] E.g. in *Digital Rights*, in which it claimed the need for a list of crimes that could justify retention.

[74] Directive (EU) 2016/681 of the 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, OJ 2016, L 119/132. The Directive has to be implemented by

Name Records at the EU level, keeps sensitive data beyond its scope.[75] Indeed, sensitive data could hypothetically be transferred to Canada if a 'precise and solid justification'[76] existed, but, and importantly, the Court of Justice considered that the need to defend public security against terrorism was not enough. This stance implied that public security was not sufficient justification *if generally considered*, as there might be *specific situations* in which it might become so. Consequently, what seems to be subject to absolute preclusion – the use of sensitive data – might instead be considered a feasible solution, albeit in very specific circumstances. This view on sensitive data was closely connected to the Court's approach to discriminatory profiling. The Court implicitly acknowledged that, by relying on individuals' sensitive data, such as religion or race, public authorities could be led to harshen measures against specific groups of people (e.g. Muslims). This would obviously result in discrimination of such groups, being targeted with counter-terrorism measures in a different manner from others.[77] The Court's stance appears prima facie to impose an absolute ban on profiling, but there are aspects that the Court did not consider and that could allow this discriminatory activity. As a matter of fact, although the use of sensitive data was undoubtedly the most blatant technique for enacting discriminatory profiling, it was not the only one. It is possible, for example, to profile people based on frequent travel destinations or food preferences. These factors do not fall within the definition of 'sensitive data', but could nonetheless be decisive to public authorities' choice to target a specific group of persons. The Court should have shed more light on these points. Nevertheless, at least in principle, the prohibition against profiling, as well as the ban on the use of sensitive data, provides some clue to the Court's attitude on the complex balance between security needs and privacy rights. And this approach is more than welcome, especially in challenging times.

Second, data should not only be processed by automated means; this should be followed by a non-automated re-examination.[78] This is a key passage and heralds a welcome and commendable stance taken by the Court against the most extreme features of surveillance tools. The Court of Justice did not blame the envisaged

Member States by May 2018. For an analysis, D. Lowe, 'The European Union Passenger Name Record Data Directive: Is it Fit for Purpose?' 16 *International Criminal Law Review* (2016) p. 78.

[75] M. Rosenfeld, 'Judicial Balancing in Times of Stress: Comparing the American, British, and Israeli Approaches to the War on Terror', 27 *Cardozo Law Review* (2006) p. 2079; A. Vedaschi, 'Has the Balancing of Rights Given Way to a Hierarchy of Values?', 1 *Comparative Law Review* (2010) p. 1.

[76] Opinion 1/15, para. 165.

[77] On profiling and its risks, R.R. Banks, 'Racial Profiling and Antiterrorism Efforts', 89 *Cornell Law Review* (2004) p. 1201; D. Barak-Erez, 'Terrorism and Profiling: Shifting the Focus from Criteria to Effects', 29 *Cardozo Law Review* (2007) p. 1.

[78] Opinion 1/15, paras. 168-174.

Agreement for being flawed on this point, as it recognised that its Article 15 provided for non-automated analysis when it was necessary to take 'decisions adversely affecting a passenger to a significant extent'. At any rate, the Court of Justice stated something crucial in relation to the automated processing phase, implying a cross-checking of data with databases containing data of suspected terrorists. The Grand Chamber remarked that such activity should be carried out through 'safe' and 'reliable' databases, limited to those used by Canada for counter-terrorism purposes. In this case, the statement of the Court is the result of a praiseworthy attitude towards individual rights, even if it failed to specify what 'safe' and 'reliable' meant in relation to databases. And this is the only objection that might be raised against the passage. Once again, concerns expressed about (purely) automatic analysis are coherent with a firm rejection of adverse decision-making based solely on automated profiling. Actually, if the whole mechanism worked automatically, measures would also be automatically taken in case of the existence of certain features, which would be detected by a technological device, without any human control. This strand of the Court's reasoning closely retraced Article 15 of Directive 95/46 – which will be replaced by Article 22 of Regulation 2016/679[79] from May 2018 onwards. Both provisions forbid resort being taken to automated decision-making for decisions affecting individuals (although some exceptions are envisaged, e.g. the subject's explicit consent). Hence, the use of automated analysis is not banned; instead, what is prohibited is using it as a basis for taking decisions. In other words, while complex algorithms are helpful for performing 'ordinary' checks on passengers, human intervention (i.e. a double check) must immediately be called into play as soon as a situation of potential risk is perceived. As a matter of fact, only human beings can verify the merits of automatic results, for example by further investigating a person's background and police record, thereby logically connecting pieces of information in a way that a machine would presumably not be able to do.

Third, Passenger Name Record mechanisms should be grounded on strong justification purposes. Consequently, stating that 'other purposes' are not well-defined,[80] the Court is particularly strict in analysing the wording of the Agreement. And this should be praised, as it is a rights-oriented approach.

Fourth, as to the retention and use of collected data – a crucial aspect of the Passenger Name Record Agreement – information on passengers who have already left Canadian territory should be stored only when there is 'objective evidence'[81]

[79] 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, and repealing Directive 95/46/EC, OJ 2016, L 119/1.

[80] Opinion 1/15, para. 181.

[81] *Ibid.*, para. 204.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press

that those passengers still present a potential risk in relation to terrorist activities and serious crime. This is a major point of the Opinion. As a matter of fact, such differentiation (among passengers before their arrival in Canada, during their stay, upon or after departure) is not provided for by the 2016 Passenger Name Record Directive. While, for certain other aspects, the Passenger Name Record Directive complies with the Court's guidelines (e.g., the prohibition against using sensitive data[82] and the need for human intervention in the processing of data[83]), this is a tricky issue. This lack of distinction could invite legal challenges to such legislation. In effect, if the Agreement had to be renegotiated according to that differentiation, whilst the Directive remained in its current form, it would be easy to envisage a differentiation depending on whether data are collected within EU territory or in non-EU jurisdictions (specifically, in Canada). Moreover, the addressed differentiation could impose the need to correlate the intelligence analysis of Passenger Name Record data with mechanisms aimed at border control.[84] Undoubtedly, the Court of Justice's reasoning is influenced by previous judgments on data retention, mainly *Digital Rights* and *Tele2* (substantively reiterating the principles set in *Digital Rights*).[85] Nonetheless, in Opinion 1/15 the Court did not merely apply previous findings. For example, in *Digital Rights* the Court of Justice quashed the provision of the Data Retention Directive leaving Member States leeway to choose between 6 and 24 months, while in this case a much longer period (five years) was deemed appropriate. Indeed, there was no contradiction: what the Court of Justice criticised in *Digital Rights* was not the length of the period per se, but the fact that specific criteria to choose between the minimum and the maximum had not been set. On the contrary, in Opinion 1/15, the retention period (five years, the same as the Passenger Name Record Directive[86]) was fixed by the Agreement and it was taken into consideration as such. Rather, what is unclear, thus potentially causing lack of legal certainty, was the standard it used to review retention periods. Furthermore, another passage deserves attention: although the Court's Opinion followed the Advocate General, on this specific point there was a subtle difference. While the Advocate General emphasised the mechanism of depersonalisation of data (i.e. masking them after 30 days), maintaining that it played a pivotal role in the safeguard of fundamental rights, the Court did not pay much attention to it, in spite of the quite long retention period. Briefly, two (slightly) different approaches to the restriction of

[82] Directive 2016/681, recital 37.

[83] *Ibid.*, Art. 12(5).

[84] As noted by R. Bossong, 'Passenger Name Records – from Canada back to the EU', *Verfassungsblog*, 28 July 2017, <verfassungsblog.de/passenger-name-records-from-canada-back-to-the-eu/>, visited 19 March 2018.

[85] *See supra*.

[86] Whose masking period is, instead, six months.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press

fundamental rights for national security reasons can be distinguished. On the one hand, the Advocate General assumed that a retention period of five years was excessive, but it could be remedied through data masking; on the other hand, the Court maintained that such a period was justifiable per se. The Advocate General's stance must be welcomed because it was more explicit and clear than the Court's approach. The Court did not explicitly address the length of retention, confining itself to a concise assertion on an issue that could cause uncertainty as to the criteria employed to rule on the retention period.

Fifth, if Canadian authorities have to disclose collected data to the authorities of a third country, an adequacy decision by the Commission regarding such a third country or an international agreement in place between it and the EU should be adopted, in order to avoid indirect circumvention of EU law principles. In this regard, the Court of Justice strongly relied on *Schrems*, which clarified the meaning of 'adequate level of protection' as 'essential equivalence'. Such a statement does not mean that the standards of data protection in the third country must coincide *in toto* with EU standards (namely, the relevant articles of the Charter and specific data protection provisions), but that at least the essence of guarantees must be comparable. Consequently, non-EU countries should conform at least to the core of EU data protection law (e.g., purpose limitation and independent oversight).

Sixth, according to the Court, data subjects should be individually notified when their Passenger Name Record data have been used and retained by the competent Canadian authority or when data are disclosed. This is another key point. Notification does not constitute a ground for data processing (as does, for instance, explicit consent), but it is an ex post guarantee, to be enacted at a later stage, i.e. when (and if) a passenger's data are processed for investigative purposes. Coherently, the Court specified that notification may take place 'as soon as this information is no longer able to jeopardise the investigations'.[87] The issue of individual notification had not been expressly addressed in detail in *Digital Rights* nor was it regulated by the Passenger Name Record Directive. Therefore, the Court's stance on the matter could represent another ground for a legal challenge to the Passenger Name Record Directive.

Ultimately, independent oversight mechanisms should be provided.[88] This caveat may cast doubts on the mechanisms set forth by the *Privacy Shield*, which has regulated the exchange of data between the EU and the US since that the previous framework, the *Safe Harbour* Agreement, was struck down as a consequence of the *Schrems* judgment. From this perspective, the Civil Liberties, Justice and Home Affairs Committee of the Parliament (LIBE) has raised concerns

[87] Opinion 1/15, para. 220.
[88] *Ibid.*, para. 228.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press

on this scheme, underlining, among other things, the insufficient independence of the body charged with oversight.[89]

In sum, not only will this Opinion have significant impact on the Passenger Name Record Directive and the *Privacy Shield*, but it could also influence other Passenger Name Record agreements, both existing (i.e. with the US and Australia) and future ones (relevantly, while this proceeding was pending, the Parliament asked for negotiations with Mexico to be stopped).[90]

From a more general point of view, this is the first time the Court of Justice has ruled on the compatibility of an international agreement with guarantees enshrined in the Charter, regarded as an autonomous legal parameter. In doing so, the Court took an important step, for two main reasons: on the one hand, this reinforced the 'constitutional' value of the Charter,[91] which was afforded the capability to function as the only parameter for deciding whether challenged acts (including international agreements) violated EU law. On the other hand, international agreements were substantively considered the equivalent, in the external dimension, of EU legislation in the internal dimension.[92] This equivalence was affirmed not only at the theoretical level of the hierarchy of sources, but also as to the practical implications of the standards to be respected. This approach reflects the supremacy of EU constitutional values, even over what has been negotiated at the international level.

Additionally, both the Parliament, in triggering the procedure, and the Court of Justice, in deciding the issue, took full advantage of the mechanism – explicitly envisaged by the TFEU – allowing challenges to an international treaty that allegedly derogates from EU law. The former sought the Court's Opinion on an Agreement that was politically and strategically crucial, given the current seemingly endless threat of terrorism. In parallel, the Parliament – perhaps due to its institutional position and, more specifically, to its role within the international treaty-making procedure – did not embrace a securitarian approach, as opposed to the Council and the Commission. Therefore, not all EU institutions that take part in (*lato sensu*) legislation-making currently let security prevail over rights. By way of its request, the Parliament strongly invited the Court of Justice to rule definitively on the merits of a Passenger Name Record agreement. As said, when it repealed the first Agreement with

[89] European Parliament, Resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-US Privacy Shield.

[90] Answer given to the European Parliament by Mr Avramopoulos on behalf of the Commission (4 November 2015). It is worth noting that negotiations may begin with Argentina and Japan as well.

[91] On the attitude of the Court of Justice, particularly in privacy-related cases, to behaving as a 'constitutional' court, *see* A. Vedaschi and V. Lubello, *supra* n 5, at p. 17.

[92] As explicitly stated by the Court of Justice, in the commented Opinion, para. 67.

the US,[93] the Court's reasoning focused exclusively on the choice of the legal basis;[94] under such circumstances, the Parliament had not relied on the Charter when it raised human rights concerns, since it merely had interpretative value in the period before the Lisbon Treaty. For its part, the Court of Justice quickly seized the opportunity to do what it had never done before, i.e. explicitly extending principles elaborated in a long series of mainstream decisions. This conveys the idea that guarantees for the rights to privacy and data protection must be affirmed on a larger scale, even in challenging times.

The Court of Justice also did something else that is worth remarking upon: in carefully analysing the text of the Agreement, even censuring its wording, it engaged in a task that could be defined as 'borderline' to that of a legislative drafting committee. The Court suggested the correct way to redraft the Agreement to other EU institutions, not only by way of principled declarations, but also by proffering concrete examples of the words and phrases to be substituted. This high rate of 'intrusiveness' can be related to the gist of this decision, which can be synthesised as follows. Conceiving a legal framework in which surveillance has no role would be utopian, given the seriousness of the current terrorist threat; nonetheless, mass surveillance must be kept subject to particularly strict rules. Against this background, if the policy-maker proves unable to remain within these limits and to guarantee that individual rights will not be totally sacrificed in the name of security, courts will be increasingly called to play a pivotal role, even going beyond their institutional attributions and bearing quasi-legislative (and political) responsibility.[95]

Conclusion

This decision has shaped the complex balance between rights and security in an increasingly detailed manner.[96] Given the growing demand for security, the Court of Justice's achievement in reconciling such competing interests appears to be the most rational and enlightened in the current circumstances. In other words, being forced to depart from a wholly pro-rights stance in favour of a more realistic one, the Court showed full mastery in reading – and, to a certain extent, redrafting – a security-related tool in a rights-oriented manner.

[93] Joined Cases C-317/04 and C-318/04.

[94] *See supra*.

[95] For a discussion of the 'creative' role of the courts, O. Pfersmann, 'Contre le néo-realisme juridique. Pour un débat sur l'interpretation', *Revue française de droit constitutionnel* (2002) p. 789 at p. 790.

[96] For more detail on how the Court approached this complex balance in the commented Opinion, *see* A. Vedaschi, 'L'Accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione europea', 62 *Giurisprudenza costituzionale* (2017) p. 1913.

The core of Opinion 1/15 lies in two (apparently opposite, but indeed compatible) features. On the one hand, the Court of Justice has definitely accepted that generalised and indiscriminate surveillance of travellers is a useful tool in the fight against terrorism. However, this securitarian attitude was wisely mitigated; the Court showed awareness of the serious risks that bulk surveillance implies for fundamental rights, in particular when clear and precise criteria for the concrete implementation of such measures are lacking.

After having examined the Opinion in detail, it is necessary to take stock of the outcome of this analysis with a view to drawing some manner of conclusion on the three points addressed in the introduction.

As to the first point, i.e. its impact on existing EU acts, as well as on those under negotiation, EU institutions are likely to renegotiate existing agreements and to take features established in the Court's Opinion into account in ongoing ones. Indeed, this might be exactly the Court of Justice's intent, as demonstrated by its willingness to involve itself in a quasi-legislative scheme, agreeing to bear quasi-political responsibility. The Parliament did not dare take such responsibility when it triggered the procedure under Article 218(11) TFEU, instead preferring to indirectly manifest its concerns about the Agreement, thereby shifting the task to the Court.

In relation to the second point, i.e. how this Opinion is positioned within the established case law of the Court, although it adheres to the same general lines of previous decisions, it undoubtedly reinvigorated and boosted previous findings. In scrutinising the EU-Canada Passenger Name Record Agreement, Opinion 1/15 has confirmed, reinforced, refined and made more specific what the Court had already stated in relation to the collection, retention and use of personal data, in at least three previous decisions.

Nevertheless, the differentiating features of this Opinion dwell in two main aspects: firstly, an increased show of confidence by the Court of Justice in dealing with highly technical matters. This is demonstrated by the fact that the Court has basically redrafted certain parts of the Agreement and showed a certain mastery in its ability to distinguish between the different timeframes in which data are retained (a level of specificity that, as remarked above, was not even envisaged by the EU lawmaker in the Passenger Name Record Directive). Secondly, it clarified that principles set in *Digital Rights*, *Schrems* and *Tele2 Sverige* (dealing with a directive, an adequacy decision on the transfer of a generality of data and national law, respectively) do extend to Passenger Name Record data as well, thus building a comprehensive framework for EU data protection, which will be highly beneficial to the perception of the EU as a rule of law-based institution.

Last but not least, with regard to the third point, i.e. the impact of this decision on the perception of the tricky balance between rights and security, the Court took a firm stance towards the protection of fundamental rights, avoiding, at the same

time, the pitfall of a utopian approach. In other words, it remained steady on the realistic assumption that, if the Western world wants to defeat terrorism, some intrusion in fundamental rights must necessarily be tolerated. As a result, the Court of Justice definitively accepted mass surveillance, albeit only to a certain extent and under strict conditions. Ultimately, this decision may help steer the lively theoretical debate on rights and security towards the awareness that promoting and safeguarding rights does not necessarily result in waiving realism.

https://doi.org/10.1017/S1574019618000202 Published online by Cambridge University Press