University of New South Wales Law Research Series

DEVELOPING A EUROPEAN STANDARD FOR INTERNATIONAL DATA TRANSFERS AFTER SNOWDEN: OPINION 1/15 ON THE EU CANADA PNR AGREEMENT

MONIKA ZALNIERIUTE

(2018) 81(6) Modern Law Review 1046
[2019] *UNSWLRS* 6

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Accepted version (pre-edited), published in *Modern Law Review*, 2018, Vol. 81, Issue 6, pp. 1046-1063, 2018.

DEVELOPING A EUROPEAN STANDARD FOR INTERNATIONAL DATA TRANSFERS AFTER SNOWDEN: *OPINION 1/15* ON THE EU-CANADA PNR AGREEMENT

BY

MONIKA ZALNIERIUTE[1]

ABSTRACT

In *Opinion 1/15* Court of Justice of the European Union (CJEU) held that the proposed EU-Canada agreement on the transfer of Passenger Name Record data (PNR agreement) must be revised before its final adoption because parts of the agreement are incompatible with EU fundamental rights framework.[2] This note argues that the real significance of the *Opinion 1/15* can only be understood in a broader historical context of an increasing securitization on international level between 09/11 attacks and Snowden revelations. In particular, *Opinion 1/15* emerges as a powerful addition to the existing data privacy trilogy established by the CJEU in the post-Snowden era in an attempt to re-balance the terms of international cooperation in data-sharing by the EU and other countries. These terms were largely modelled around national security interests that have gained significant prominence in the aftermath of the 9/11 events. While the pro-securitization policies have indeed been very successful in gaining support among different private and public actors, e.g., in handling passenger name records (PNR) or personal data in financial transfers (SWIFT), it is however questionable whether CJEU's pushback – without the political support of EU Commission and Member States - will receive similar success on international level any time soon.

INTRODUCTION

The new international momentousness of data privacy can hardly go unnoticed, and it seems that everyone is talking about this perplexing and puzzling area of international law and international relations. Indeed, the significance of 'data privacy momentum' inspired by the Snowed revelations of 2013 is still unfolding five years after and numerous 'wars',[3] 'battles',[4]

[1] Postdoctoral Fellow, Allens Hub for Technology, Law, & Innovation, UNSW Sydney, Australia. The author is grateful for insightful comments and constructive feedback that Megan Richardson and anonymous reviewers provided on earlier drafts. The author is also grateful for the continuous support and encouragement from Sandra Amanka.

[2] Opinion 1/15 of the Court of Justice of European Union, (ECLI:EU:C:2017:592) available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=558533, visited 23/01/2018.

[3] Farrell, Henry, and Abraham Newman. "The Transatlantic Data War: Europe Fights Back Against the NSA." *Foreign Aff.* 95 (2016): 124;

[4] Hare, Stephanie. "For your eyes only: US technology companies, sovereign states, and the battle over data protection." *Business Horizons* 59.5 (2016): 549-561;

'fights', 'tensions',[5] and 'Great Games'[6] over data privacy between various actors in international arena are more visible than ever. Far-reaching manifestations of international disagreements over data privacy regulation, such as European Court of Justice's (CJEU) invalidation of the US-EU *Safe Harbour* agreement,[7] the (in)famous 'right to be forgotten' case decided in *Google vs Spain*,[8] the creation of the new *Privacy Shield* agreement,[9] the potential overthrow of the standard contractual clauses in the currently unfolding *Schrems II* saga,[10] are emerging one after another. In this politically charged transatlantic climate, the EU judicature was requested by the EU European Parliament (EP), pursuant to Article 218(11) TFEU, to ascertain whether the proposed EU-Canada agreement negotiated in 2014 on the transfer of Passenger Name Record data (PNR agreement) was compatible with primary EU law and, in particular, with the rights to respect for private life and the protection of personal data guaranteed by Articles 7 and 8 of the EU Charter of Fundamental Rights (EUCFR).[11] The *Opinion 1/15*, delivered on the 26th July 2017 by the Grand Chamber of the CJEU in response to this request, is a ground-breaking example of law-making, with important implications for many areas of EU law, the future of the EU legal framework for PNR, as well as international data transfers and transatlantic data relations more generally.

It is impossible to discuss all the different aspects of this judgment in the limited space provided. Instead, this comment argues that the real significance of the *Opinion 1/15* can only be understood in a broader historical context of an increasing securitization on international level between 09/11 attacks and Snowden revelations. The case note adopts an interdisciplinary lens of *international law and international relations*[12] to better understand the so-called 'legal politics' and institutional preferences of different actors in transatlantic data privacy landscape. While international law and political science disciplines are still quite distant because they are organized around distinct goals and addressed at different audiences, nonetheless, there is a substantial and burgeoning intersection between the two.[13] In particular, the article relies on *historical institutionalism*[14] which emphasizes the importance of time and timing (also called

---

5 Lee A. Bygrave, 'Transatlantic Tensions on Data Privacy', 3–4, 6 (Transworld, Working Paper No. 19, 2013).

6 Greenleaf, Graham, 'International Data Privacy Agreements after the GDPR and Schrems' (January 30, 2016) 139 *Privacy Laws & Business International Report* 12-15; *UNSW Law Research Paper* No. 2016-29, https://ssrn.com/abstract=2764864, p. 8.

7 Case C-362/14, *Schrems v. Data Prot. Comm'r*, 2015 E.C.R. I-627.

8 Case C-131/12 *Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, 13 May 2014.

9 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance) *OJ L 207, 1.8.2016, p. 1–112*.

10 'Schrems Busts Privacy Shield Wide Open,' *The Register*, 3rd October 2017, https://www.theregister.co.uk/2017/10/03/schrems_busts_privacy_shield_wide_open/, visited 06/10/2017.

11 Charter of Fundamental Rights of the European Union (OJ 2010 C 83/389).

12 Keohane, R., International Relations and International Law: Two Optics, 38 *Harv. Int'L L.J.* 487 (1997). Slaughter, A-M, Tulumello, A. & Wood, S., 'International Law And International Relations Theory: A New Generation of Interdisciplinary Scholarship,' 92 *AJIL* 367 (1998), Abbott, K., 'Toward A Richer Institutionalism For International Law And Policy,' 1 J. *Int'l L.& Int'l Rev.* 9 (2005).

13 Dunoff, J., and Pollack, M. (eds.), *Interdisciplinary Perspectives on International Law And International Relations: State Of The Art*, CUM, 2012; Hafner-Burton, E.M., Victor, D.G. and Lupu, Y., 'Political Science Research in International Law: The State of the Field,' *The American Journal of International Law*, 2012, Vol.106(1), pp. 47 -97.

14 Steinmo, S., 'What is Historical Institutionalism?' in Della Porta, D. and Keating, M., (eds) *Approaches in The Social Sciences*, CUM, 2008.; Thelen, K. and Steinmo, S., 'Historical Institutionalism in Comparative Politics' in Steinmo, S., Thelen, K., and Longstreth (eds), *Structuring Politics: Historical Institutionalism in Comparative Analysis*, CUM, 1992; Farrell, H., Newman, 'Making Global Markets: Historical Institutionalism in International Political Economy,' *Review of International Political Economy* 17(4) (2010).

process tracing or sequencing) in causal process, to demonstrate that *Opinion 1/15* emerges as a powerful addition to the existing data privacy trilogy established by the CJEU in the post-Snowden era in an attempt to re-balance the terms of international cooperation in data-sharing by the EU and other countries. Part I of this note provides background and outlines the context and content of the EU-Canada PNR Agreement. Part II focuses on the CJEU's *Opinion 1/15* and explains its reasoning. Part III evaluates the Opinion, arguing that it contributes to a further constitutionalisation of data privacy in EU legal order. Part IV discusses the implications of the CJEU's judgment from a broader, global perspective, considering its implications for the EU's PNR regime as well international data transfers more generally.

1. FACTUAL AND LEGAL BACKGROUND

Passenger name records (PNR) data is information provided by passengers when they book tickets and check in for flights, and may include the names, addresses, payment and credit card details, seating and luggage information, as well as any special dietary requirements of the passengers, which may reveal religious beliefs. While the PNR data is primarily collected for commercial purposes by the air carriers, since the 9/11 attacks in 2001 it has been increasingly regarded as a useful risk assessment tool by law enforcement authorities tasked to fight serious crime and terrorism.

The draft EU-Canada PNR agreement is neither the first nor the only international agreement requiring PNR data transfers from EU to third country. The PNR agreements came into being shortly after 9/11, when the US Congress adopted a series of legislative measures directed at the fight against terrorism;[15] and air carriers were required to provide the US authorities with access to the PNR data stored in their databases.[16] However, the clash between the US 'anti-terror' legislation requirements and data protection principles in the EU soon became apparent. Thus, in 2004 the EU agreed to share transatlantic flight PNR data with the US Customs Service, which in turn assured an 'appropriate handling' of passenger records.[17] This agreement was annulled by the CJEU in 2006 for having the wrong legal basis.[18]

At the same time, it has to be noted that the governments of EU Member States were also a actively contributing to the development of securitization policies in response to their own experiences of terrorism in the mid-2000s. In particular, the London bombings in 2005 led the UK government to be one of the main driving forces behind the development of surveillance and transatlantic data-sharing framework.[19] Soon after 9/11, the growing perception of the transnational danger of terrorism led US and EU security experts to create a High Level Contact Group to lay the groundwork for a more formal EU-US deal on data sharing for surveillance

---

15 Most prominent example being the '*Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act'* (P.A.T.R.I.O.T. Act) of 2001 (H. R. 3162) which Preamble reads: *"[T]o deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."*

16 Pursuant to the *Aviation and Transportation Security Act (ATSA)* of November 19, 2001, as well as the *Enhanced Border Security and Visa Entry Reform Act (EBSV)* of May 5, 2002.

17 The 2004 Agreement between the European Community and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (O.J. 2004, L 183/84) See Commission, Communication from the Commission to the Council and the Parliament, '*Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach,'* December 16, 2003, COM (2003) 826.

18 Joined cases C-317/04 and C-318/04 *European Parliament v Council* (C-317/04) *and Commission* (C-318/04) [2006] ECLI:EU:C:2006:346, paras. 67 – 70.

19 Svendsen, Adam DM. "On 'a Continuum with Expansion'? Intelligence Cooperation in Europe in the Early Twenty-first Century." *Journal of Contemporary European Research* 7.4 (2011): 520-538.

purposes, which could 'over time tilt the EU's balance away from what they saw as excessive privacy concerns and towards national security'.[20] Although there was an initial disagreement within the EU after 9/11 between the civil rights-oriented officials and security officials, the latter eventually came to dominate transnational negotiations, passing a series of new laws and engaging in practices that seriously compromised the aspirations of the newly adopted EUCFR.[21]

Because the development of surveillance and data sharing frameworks depends on great levels of technological capacity, international cooperation in data-sharing and surveillance is just as much about technology, as it is about geopolitics.[22] Therefore, the need for cooperation and exchange of technological capacity resulted in a strong anti-terrorism rhetoric[23] and environment, which in turn led to numerous data-sharing and cooperation agreements. In particular, since the mid-2000s the USA and EU have agreed between themselves on data protection principles for information shared for law enforcement purposes,[24] and initiated numerous other data-invasive measures, such as *Data Retention Directive* (now invalidated), and the Council of Europe's *Convention on Cybercrime.*[25] It is in this context that the EU PNR agreements with other countries came into being. Currently, the EU has signed agreements with the United States,[26] Australia,[27] and Canada,[28] but numerous other countries have also expressed interest in negotiating PNR agreements with the EU.[29]

---

[20] Farrell, Henry, and Abraham L. Newman. 2014. "The New Politics of Interdependence: Cross- National Layering in Trans-Atlantic Regulatory Disputes". *Comparative Political Studies* 48: 497- 526, p. 11.

[21] For a detailed account of the interactions between different officials in the EU after the 9/11, see Farrell and Newman. 2014. *The New Politics of Interdependence,* pp. 505 – 510. For a detailed discussion of surveillance laws in EU, see Reidenberg, Joel R. 2014. 'The Data Surveillance State in the United States and Europe' *Wake Forest Law Review* 49: 583-608, at 592.

[22] I am grateful to anonymous referee for this point. For a detailed analysis of technology risks for privacy, see, Caire, Patrice, Assaad Moawad, Vasilis Efthymiou, Antonis Bikakis, and Yves Le Traon. "Privacy challenges in Ambient Intelligence systems." *Journal of Ambient Intelligence and Smart Environments* 8, no. 6 (2016): 619-644.

[23] For a detailed account, see Michaelson, Christopher, "Balancing Civil Liberties Against National Security? A Critique of Counterterrorism Rhetoric" *University of New South Wales Law Journal.* (2006) 29(2) 13.

[24] See, e.g., *Statement on Information Sharing and Privacy and Personal Data Protection between the European Union and the United States of America*, 13 December 2008, /http://www.dhs.gov/xlibrary/assets/usa_statement_data_privacy_protection_eu_12122008.pdf/.

[25] ETS No.185. Although the Convention was drafted before the 9/11 events, they have strongly influenced the Convention's future and the additional protocols.

[26] See Agreement between the United States of America and the European Union of 2012 on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJ L 215, 11.8.2012, p. 5–14.* See also Council Decision 2012/472/EU of 26 Apr. 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ 2012 L 215/4. For more information on the EU-US PNR storyline, see Suda, Y., 'Transatlantic Politics of Data Transfer: Extraterritoriality, Counter-Extraterritoriality and Counter-Terrorism,' *Journal of Common Market Studies* 51.4 (2013): 772-788.

[27] See Council Decision 2012/381/EU of 13 Dec. 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186/3.

[28] The first EU-Canada PNR Agreement (see 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/Passenger Name Record data, OJ 2006 L 82/14) expired in Sept. 2009. The new envisaged agreement was subjected to review in Opinion 1/15.

[29] See, e.g, European Commission, Statement/15/5374, 'Beginning of negotiations between Mexico and the European Union on PNR data transmission', 14 July 2015. A reference to the requests submitted by the United Arab Emirates, South Korea, Brazil, Japan and Saudi Arabia is made in a question to the European Commission filed by a member of the European Parliament (Janice Atkinson) on 11 June 2015 (E-009612-15).

One of such EU agreements with Canada expired in 2009,[30] and the new PNR agreement was signed in 2014, after lengthy negotiations. The envisaged EU-Canada agreement, (which is the subject of Opinion 1/15) requires airlines operating in EU to systematically transfer PNR data to Canadian authorities. The agreement stipulates the transfer of the PNR data for Canadian authorities to use and retain, with a possibility of transfer subsequently to other authorities and to other non-member countries, for the purpose of combating terrorism and forms of serious transnational crime. To that end, the envisaged agreement provides, *inter alia,* for a data storage period of five years and lays down requirements in relation to the PNR data security and integrity, immediate masking of sensitive data, rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The Council of the EU requested the EP's approval, which suspended the procedure to conclude the agreement, and decided to refer the matter to the CJEU, pursuant to Article 218(11) TFEU, in order to ascertain whether the envisaged agreement was compatible with primary EU law and, in particular, with provisions relating to respect for private life and the protection of personal data, as guaranteed by Articles 7 and 8 of the EUCFR.

A great amount of far-reaching 'pro-security' legislation and data-sharing agreements have been implemented without any serious democratic debate during the decade following 09/11, and only some received *post factum* attention by raising suspicions about their *constitutional* legitimacy in the US and EU.[31] However, the PNR agreements as well as other data sharing agreements, such as SWIFT[32] and Europol-USA[33] agreement have involved significant controversies over USA's ability to protect the personal information of EU citizens.[34] In consequence, the EP used its novel powers granted under Lisbon Treaty to engage the CJEU in *ex ante* review of the draft EU–Canada agreement. In light of the EU's adoption of the *PNR Directive* back in 2016,[35] and the so-called 'Snowden momentum', the Opinion has attracted a lot of interest among governments, airlines and data privacy advocates.

2. OPINION OF THE COURT

30 See n 28.

31 See Scheinin, Martin. *et al.*, '*Law and Security. Facing the Dilemmas'*, EUI Working Papers Law 2009/11, available at /cadmus.eui.eu/handle/1814/12233/, (visited 06/10/2017). Some of investigative measures were also declared to be in breach of the European Convention of Human Rights by the ECtHR, see, e.g., *S. and Marper v UK* [2008] ECHR 1581*Bykov v. Russia,* [2009] ECHR, App. No. 4378/02,

32 The SWIFT saga has two agreements concluded in 2009 and 2010; see *Agreement between the European Union and The United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program* (O.J. 2010, L 8/11) and *2010 SWIFT Agreement* (O.J. 2010, L 195/5). See also Pfisterer, V., The Second SWIFT Agreement between The European Union and the United States of America – An Overview, 2010, 11 *German Law Journal* 1173-1190.

33 See the *Agreement between the United States of America and the European Police Office (Europol)* of and *Supplemental Agreement between Europol and the USA on Exchange of Personal Data and Related Information, at* /https://www.europol.europa.eu/sites/default/files/flags/supplemental_agreement_between_europol_and_the_usa_on_exchange_of_personal_data_and_related_information.pdf/ visited 02/06/2014.

34 For a discussion, see Ruddy, T. F. (2014). 'Regimes Governing the Re-use of Personal Data in the US and the EU: a Primer on Mass Surveillance and Trade,' *The Transatlantic Colossus: Global Contributions to Broaden the Debate on the EU-US Free Trade Agreement.*

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

On the 26th July 2017, the Grand Chamber of the CJEU issued *Opinion 1/15* that the proposed EU-Canada agreement on the transfer of Passenger Name Record data (PNR agreement) must be revised before its final adoption because parts of the agreement are incompatible with EU fundamental rights framework.[36] The CJEU commenced by recalling that international agreements entered into by the EU form an integral part of the EU legal system and therefore such agreements must be 'entirely compatible with the Treaties and with the constitutional principles stemming therefrom.'[37]

Firstly, the CJEU focused on the appropriate legal basis for the proposed agreement, as the EP had referred a question whether the envisaged agreement should be based on Article 82 TFEU (judicial cooperation in criminal matters) and Article 87 TFEU (police cooperation) or Article 16 TFEU (protection of personal data). Following the opinion of Advocate General Mengozzi, the CJEU noted that Article 82 TFEU (judicial cooperation in criminal matters) was not an appropriate legal basis for the agreement because judicial authorities were not included in the proposed agreement. The Court found that the envisaged agreement had two interlinked objectives: safeguarding public security and safeguarding personal data and thus had to be concluded on the basis of both Article16 TFEU and Article 87 TFEU.[38]

The CJEU then held that the transfer of the PNR data from the EU to Canada, and the rules laid down in the PNR Agreement, violated the fundamental rights to respect for private life and to protection of personal data in Articles 7 and 8 EU Charter. The Court first held that the proposed agreement constituted a serious interference with these fundamental rights guaranteed by the Charter.[39] As a result, the CJEU subjected the proposed agreement to a strict review standard of compliance and elaborated in detail how the agreement had to be amended to ensure its compliance with the fundamental EU law.

In particular, the CJEU examined whether the interferences could be justified in accordance with Article 52(1) EUCFR.[40] It noted, in this respect, that the interferences in question were justified by the pursuit of an objective in the general interest, namely 'to ensure public security by means of transfer of PNR data to Canada and the use of that data within the framework of the fight against terrorist offences and serious transnational crime'.[41] The CJEU held that the envisaged agreement was appropriate for the purposes of ensuring that that objective was achieved.[42]

The weaknesses of the proposed agreement however became apparent as regards the proportionality of the interferences, which must be 'limited to what is strictly necessary'.[43] The Court considered that several provisions of the envisaged agreement did not lay down sufficiently clear specification of what personal data was requested.[44] The CJEU referred to the newly adopted *EU PNR Directive* as a relevant benchmark for assessing the proposed PNR agreement and found that the provisions on the transfer of *sensitive* data to Canada did not

---

36 Opinion 1/15 of the Court of Justice of European Union, (ECLI:EU:C:2017:592) available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=558533, visited 16/10/2017.

37 Opinion 1/15, para 37.

38 Opinion 1/15, para. 90.

39 Opinion 1/15, paras. 127-129.

40 Opinion 1/15 para. 136.

41 Opinion 1/15, paras. 148-149.

42 Opinion 1/15, paras. 152-153.

43 Opinion 1/15, para. 154.

44 Opinion 1/15. paras. 157-158.

provide sufficient protections, as required by the Charter under Articles 7, 8 and 52(1) in combination with Article 21 of EUCFR on non-discrimination.[45] The *General Data Protection Regulation* ('GDPR')[46] which replaced the *Data Protection Directive*[47] on 25 May 2018, defines sensitive data as **'**data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.'[48] Previously, the Data Protection Directive defined it as 'data about "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, health, and sex life." The CJEU therefore used an opportunity to highlight that 'sensitive data' is a special category of data in EU law that should receive especially stringent protections. The Court also made a distinction between the transfer and storage of PNR data for the purposes of *entering* Canada,[49] and usage and retention of data of all passengers after they have *departed* Canada.[50] It considered that the five-year data retention period of *all* the passengers after they departed Canada[51] and potential disclosure of the PNR data by Canadian authorities to third countries[52] or individuals[53] was not limited to what is strictly necessary. Therefore, the CJEU declared that these provisions were incompatible with fundamental rights and thus the envisaged agreement may not be concluded in its current form.

The Court, however, did not stop at this point. Unusually, it went to specify in detail how the proposed EU-Canada PNR agreement should be 'revised': that it should specify clearly the manner the PNR data is to be transferred to Canada; that it should ensure the reliability and non-discriminatory nature of the models and criteria used in automated processing of PNR data; that agreement must assure the limited use of database; ensure the independent oversight of data sharing with other bodies; limit PNR data retention after passenger's departure; ensure that any disclosure of PNR data to the governments of third countries is subject to either an agreement between EU and those countries or 'adequacy' decision; ensure the right individual notification for air passengers in the event of use of PNR data concerning them; and guarantee the supervision by independent supervisory authority.[54] By specifying this criteria, the court indicated how *any* PNR agreements should be drafted to ensure their compatibility 'with the treaties and with the constitutional principles stemming therefrom.'[55]

---

45 Opinion 1/15, para. 166-7. Processing of sensitive data is prohibited under Articles 6(4), 7(6) and 13(4) of the EU PNR Directive.

46 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 (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1–88*.

47 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.

48 Article 9 of GDPR.

49 Opinion 1/15, paras. 188-189.

50 Opinion 1/15, paras. 200-202.

51 Opinion 1/15, paras. 206-207.

52 Opinion 1/15, paras. 213-214.

53 Opinion 1/15, paras. 216-217.

54 Opinion 1/15, para. 232.

55 Opinion 1/15, para. 67.

3. CONSTITUTIONALISATION OF DATA PRIVACY IN EU: DEVELOPING A STRICT STANDARD

Opinion 1/15 is the fourth in a what has now turned into a 'quadrilogy' of data protection cases on bulk-data collection for security purposes following the CJEU's earlier judgments in *Digital Rights Ireland*,[56] *Schrems*,[57] and *Tele2 Sverige*.[58] In landmark ruling of *Digital Rights Ireland*, the CJEU invalidated Directive 2006/24/EC ("the Data Retention Directive"), on the grounds that it represented a disproportionate and unjustified interference with Articles 7 and 8 EUCFR. While the concerns about and challenges to Data Retention schemes in EU and Member States pre-date Snowden revelations (indeed, data protection and privacy advocates, DPAs as well the EU Parliament have long been concerned about the data retention schemes (as well as PNR, SWIFT and other regimes),[59] this case note argues that the post-Snowden policy climate enabled the CJEU to be more receptive to those concerns than in the pre-Snowden era. Indeed, in the aftermath of Edward Snowden's revelations, the CJEU further expanded on the limits on the bulk-data collection programs in two additional significant ruling. Firstly, in *Schrems* the CJEU invalidated the EU Commission's decision on adequacy of data protection provided by the Safe Harbour agreement, which allowed the transfers of personal data from the EU to US for 15 years between 2000 and 2015. In subsequent *Tele2 Sverige*, the CJEU followed its approach in *Digital Rights Ireland* and extended this to national data retention regimes in Member States. In this context, the *Opinion 1/15* presented the Court with yet another opportunity to articulate data protection requirements for international data transfers in the context of the international PNR agreement between the EU and Canada.

In light of the data protection trilogy in *Digital Rights Ireland-Schrems-Tele2 Sverige*, as well as serious concerns about the envisaged agreement expressed by the European Data Protection Supervisor[60] (being concerns that were ignored by the Council of the EU), an adverse CJEU's opinion on the proposed EU-Canada PNR agreement hardly comes as a surprise. *Opinion 1/15* was fully consistent with the recent post-Snowden case-law, however, it also went beyond it and elaborated more detailed requirements for the transfers of personal data to third countries and for the first time ruled on the compatibility of a draft international agreement with the fundamental rights under the Charter.

In particular, the CJEU found that transfers of *sensitive* personal data outside the EU require required '… a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime' (para 165), and the proposed agreement failed to provide 'such justification' (para. 165). This novel point was not elaborated by the Court in the earlier cases, and *Opinion 1/15* points to a very strict requirement of a 'solid justification' for the transfers of *sensitive* personal data from the EU to third countries. Similarly, the high level of independence required by the Court for the

---

56 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* [2014] E.C.R. I-238.

57 Case C-362/14, *Schrems v Data Protection Commissioner* EU:C:2015:650,

58 Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Postoch telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970 *(Tele2 Sverige)*

59 For a detailed account, see Kosta, Eleni. "The way to Luxemburg: national court decisions on the compatibility of the data retention directive with the rights to privacy and data protection." *SCRIPTed* 10 (2013): 339.

60 EDPS, Opinion on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data, 30/09/2013, https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf, visited 16/10/2017.

authorities supervising the implementation of data sharing agreements[61] suggests that CJEU has now developed a principled position on the appropriate limits of bulk collection of personal data and transfers of personal data to third countries, from which it is unlikely to depart in any near future.

The *Opinion 1/15* thus fits very well among a number of recent far-reaching CJEU judgments delivered since 2013 and the policy shock created by Snowden revelations which shifted an international data privacy discourse, and, in turn, resulted in a series of CJEU judgments that are much less tolerating of the securitization and surveillance measures than in the pre-Snowden era. These surveillance judgments, along with the (in)famous Google Spain case might be seen as a European overreach in response to Snowden leaks, and they certainly have been perceived this way by the powerful US tech companies,[62] and the US Government.[63] The CJEU's decision in *Google Spain* did not concern surveillance measures, but rather de-listing on search engines, but it can also be interpreted as a part of the CJEU's pushback (albeit indirect) against the secret mass-surveillance programmes because Snowden revealed that the commercial data exchanges taking place on US tech companies infrastructure, such as e-mail and social media platforms, were secretly leveraged for mass-surveillance by the US government. Therefore, as noted by Henry Farrell, even if there has been an overreach by the CJEU, that overreach comes in response to 'US overreach.'[64] Recent constitutionalization of data privacy by the CJEU in the mass-surveillance saga of *Digital Rights Ireland*, *Schrems* and *Tele 2*, as well as *Opinion 1/15*, should be therefore understood within a broader context of CJEU's data privacy-pushback against mass surveillance policies both within the EU and in transatlantic relations. It is argued here that it is precisely the policy shock created by Snowden revelations that provided the CJEU with an opportunity to 'reinvent' itself as a main defender of fundamental right to data privacy in EU and transatlantic relations. Indeed, the timing supports this. It did not take long after Snowden revelations for the CJEU to invalidate the *Safe Harbour* agreement; and the fate of the popular standard contractual clauses also seems to be very shaky in the light of the *Schrems II* case. The pushback by the CJEU therefore can be understood as a signal that at least the CJEU will no longer accept the rules of the game for data sharing modelled around security interest in the previous decades.

A joint approach of international law and international relations provides means to understand how those 'rules of the game' were set during the period between 9/11 and the Snowden revelations. In particular, historical institutional analysis and process tracing methodology, which emphasizes the role of timing, allows us to grasp how data privacy as a policy issue has been transformed and redefined from primarily (or nearly solely) a commercial issue in both the EU and USA into a security and surveillance issue between 2001 and 2013. For instance,

---

61 Opinion 1/15, paras. 200-202.

62 E.g, immediately after the Google Spain judgment, Google's executive Eric Schmidt stated that 'Google believes, having looked at the decision which is binding, that the balance that was struck was wrong', see Antani, Ravi. "The Resistance of Memory: Could the European Union's Right to Be Forgotten Exist in the United States." *Berkeley Tech. LJ* 30 (2015): 1173, at p. 1179-1180, quoting Gibbs, Samuel, 'Eric Schmidt: Europe struck wrong balance on right to be forgotten', The Guardian, https://www.theguardian.com/technology/2014/may/15/google-eric-schmidt-europe-ruling-right-to-be-forgotten, visited 08/10/2017.

63 E.g, US Secretary of Commerce Penny Pritzker said the Obama Administration was "deeply disappointed" in the CJEU decision and that it "necessitates release of the updated Safe Harbor Framework as soon as possible", see Department of Commerce, "Statement from U.S. Secretary of Commerce Penny Pritzker on European Court of Justice Safe Harbor Framework Decision," October 6, 2015.

64 Henry Farrell, Abraham Newman, Forget Me Not: What The EU's New Internet Privacy Ruling Means For The United States, May 19 2014, *Foreign Affairs* (2014), https://www.foreignaffairs.com/articles/united-states/2014-05-19/forget-me-not, visited 08/10/2017.

the EU Data Protection Directive was adopted on Internal Market legal basis back in 1994, and thus was treated as an aspect of economic integration aimed at preserving Single market within the EU.[65] In the USA, data privacy responsibilities laid with the US Department of Commerce, and data privacy rules were framed as an obstacle to e-commerce from the early days of the Internet.[66] The process tracing and emphasis on timing points how transatlantic data privacy policy negotiations after 9/11 have moved from DG Internal Market and the US Department of Commerce to security officials and interior ministers in the EU[67] and the Department of Homeland Security and Treasury in the US.[68] Such policy redefinition or securitization of data privacy is also evidenced by the fact data flows of commercial nature, such as airline passenger or SWIFT information exchange have been leveraged and increasingly used for national security purposes since 9/11. Therefore, the CJEU's data privacy pushback is not simply or solely against the US surveillance policies, but rather against the transatlantic securitization and mass-surveillance, which was also embraced by the EU and Member States during the period between 9/11 and Snowden revelations. Whether the court's pushback and resulting data privacy constitutionalisation in the EU legal order is likely to have any substantial impact in international relations in data privacy is yet another question.

4. IMPLICATIONS OF *OPINION 1/15* – REAL CHANGE OR YET ANOTHER ILLUSION?

The CJEU's *Opinion 1/15* not only contributes to asserting the fundamental role of data privacy in EU legal order. It may also have significant consequences for the EU's PNR scheme, as well as international data transfers and negotiations of future international agreements.

Firstly, the ruling will have significant implications for the recently adopted EU PNR Directive, and may also impact other PNR agreements by the EU with USA and Australia, as well as the related ongoing negotiations with Mexico. Civil society organizations in the EU have argued that the proposed EU-Canada PNR agreement was 'the least restrictive of all of the EU's PNR agreements' and therefore, EU has to suspend the agreements with the USA and Canada to respect the CJEU's opinion.[69] While the implications of the Opinion 1/15 for the PNR agreements are potentially wide-ranging, some may argue that the CJEU did not go far enough to challenge the very rationale of PNR schemes as a whole.

Indeed, the European Parliament, European Data Protection Supervisor and civil society organisations have long been in particularly strong opposition to EU Commission's approach to data sharing agreements for law enforcement purposes, which they argue often

---

65 See, e.g., Pearce, Graham, and Nicholas Platten. "Achieving personal data protection in the European Union." *JCMS: Journal of Common Market Studies* 36.4 (1998): 529-547.

66 See, e.g, the Clinton Administration's 'Framework for Global Electronic Commerce', 1997, available at the US White House archives, of https://clintonwhitehouse4.archives.gov/WH/New/Commerce/index.html, visited 01/08/2018.

67 In the EU, even though security officials and interior ministers have been heavily involved in transatlantic data protection negotiations since 9/11, data protection was formally transferred from DG Internal Market to DG Justice and Home Affairs in March 2005.

68 For the US, see Zarate, Juan. *Treasury's war: The unleashing of a new era of financial warfare*. Hachette UK, 2013.

69 Reuters, *Top EU court says Canada air passenger data deal must be revised,* https://ca.reuters.com/article/topNews/idCAKBN1AB0T9-OCATP, visited 16/10/2017.

fundamentally violate the principles of the EU data privacy regime.[70] For example, in stark contrast to the EU Commission's official position, the European Data Protection Supervisor has long argued that the PNR schemes, including the adequacy decisions, international agreements as well as the most recent EU PNR Directive, are not strictly necessary to fight terrorism, disproportionate to the aims pursued, and of questionable effectiveness.[71] In their latest Opinion on the EU PNR Directive, the EDPS strongly argued that "the non-targeted and bulk collection and processing of data of the PNR scheme amount to a measure of general surveillance"[72] and, lacking empirical unambiguous evidence that such a regime is necessary, the PNR Directive violates Articles 7, 8 and 52 of the Charter, Article 16 TFEU and Article 8 ECHR.[73]

Similarly, Article 29 Working Party also has a long tradition in questioning the very rationale and utility of the PNR systems. For instance, back in 2010 in its Opinion 7/2010, the WP claimed that "the usefulness of large-scale profiling on the basis of passenger data must be questioned thoroughly, based on both scientific elements and recent studies"[74] and maintained no satisfactory evidence exists proving necessity of such systems.

In contrast to such approach questioning the very essence of PNR regimes, the CJEU however, has adopted a milder stance. CJEU's approach was based on the opinion of AG Mengozzi who accepted that the PNR schemes in general – even though they may involve indiscriminate targeting and profiling, and could lead to *serious interferences* with fundamental rights – may be nonetheless compatible with fundamental rights in the EU.[75] This is in contrast to the CJEU's ruling in *Schrems* where access to the content of electronic communications on generalised basis was held to compromise the *essence* of the fundamental right.[76] The Court thus, distinguished the mass-surveillance regime in *Schrems* from the PNR data collection and

---

70 *See, e.g.*, Article 29 Working Party, *Opinion 5/2007 on the Follow-up Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security Concluded in July 2007* (Aug. 17, 2007), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp138_en.pdf; *Letter from Article 29 Working Party to Member of the LIBE Committee of the European Parliament, Brussels*, Ref. Ares (2012)15841-06/01/2012; European Data Protection Supervisor, *Opinion on the Proposal for a Council Decision on the Conclusion of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the US State Department of Homeland Security, 2012/C 35/03 (September 2nd 2012).*

71 For the latest EDPS opinion on PNR issues, see EDPS, *Opinion 5/2015 on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, 24/09/2015, https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf, visited 23/01/2018; and EDPS, *Opinion of the European Data Protection Supervisor on the Proposals for Council Decisions on the conclusion and the signature of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data*, 30/09/2013, https://edps.europa.eu/sites/edp/files/publication/13-09-30_canada_en.pdf, visited20/08/2018.

72 EDPS, *Opinion 5/2015*, para. 63.

73 EDPS, *Opinion 5/2015*, para. 64.

74 Article 29 Working Party, Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, 12 November 2010, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf, visited 23/01/2017.

75 See, e.g, Gabriela Zanfir-Fortuna, *Analysis of the AG Opinion in the "PNR Canada" Case: unlocking an "unprecedented and delicate"* matter, https://pdpecho.com/2016/09/12/analysis-of-the-ag-opinion-in-the-pnr-canada-case-unlocking-an-unprecedented-and-delicate-matter/, visited 23/01/2018.

76 *Schrems*, para. 94.

retention, which amounted to serious breach – rather than a compromise of an essence - of fundamental right.[77]

Implications for International Agreements: Parameters for Legal Basis

Moreover, beyond PNR, the questions arise with regard to other international agreements in the law enforcement area, such as the recently adopted EU-US Umbrella Agreement,[78] which is both similar and different compared to the PNR agreements. Whatever the differences in substance among these agreements might be, one thing that the CJEU made clear in *Opinion 1/15* is that all of the data sharing agreements for law enforcement purposes will have to based on Articles 16(2) (right to data protection) and 87(2) (police cooperation in criminal matters) of the TFEU. Until *Opinion 1/15*, these various instruments were adopted without Article 16 TFEU (data protection) as a legal basis, based on the view that police and/or judicial cooperation plaid a more significant role, and thus, data sharing agreements for law enforcement should be based on Article 82(1) and Article 87(2) TFEU. This is the case not only for the international PNR agreements, but also, recent EU legal instruments establishing elaborate data protection regimes, such as for example, the *EU PNR Directive* (based on Article 82(1) and Article 87(2)(a) TFEU, provisions on police and judicial cooperation in criminal matters) and *Europol Regulation*[79] (based on Article 88 TFEU, provision on police cooperation).

By articulating that Article 16(2) TFEU on data protection, in conjunction with Article 87(2), was appropriate joint legal basis for PNR agreements, the CJEU has departed from its limited (in)famous pre-Lisbon Treaty 2006 PNR ruling which held that the relevant EU-US PNR agreement fell within the framework of public security and that it was not necessarily a data protection instrument. [80] In this regard, *the Opinion 1/15* illustrates the impact of the Lisbon Treaty, which consolidated the former First and Third Pillars of the Maastricht Treaty. This is of particular significance, as noted by Hielke Hijmans, as DG Home of the European Commission will no longer be the sole negotiator of such agreements, and DG Justice will have to be equally involved in the process. [81] In this way, *Opinion 1/15* reveals how Lisbon Treaty gives more weight for data protection in the process of negotiation and adoption of such dual-goal data sharing instruments, as well as their supervision by an independent data privacy commissioner after the adoption.[82]

Implications for International Data Transfers

The *Opinion 1/15* may also impact personal data transfers outside the EU more generally, not just international agreements, including the post-Brexit UK. In this context, important questions arise whether the US *Privacy Shield* or other data transfer mechanisms, such as the

---

77 See Maja Brkan, 'In Search of the Concept of Essence of EU Fundamental Rights Through the Prism of Data Privacy' (Maastricht Faculty of Law Working Paper No 2017-01, 16 January 2017) <https://ssrn.com/abstract=2900281> accessed 7 September 2017.

78 (OJ L 336, 10.12.2016, p. 3–13)

79 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] L 135/53.

80 Joined cases C-317/04 and C-318/04 *European Parliament v Council* (C-317/04) *and Commission* (C-318/04) [2006] ECLI:EU:C:2006:346, para. 58 and paras. 67 – 70.

81 Hijmans, Hielke. "PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators." *European Data Protection Law Review* 3.3 (2017): 406-412, at 411.

82 Article 16(2) TFEU and Article 8(3) of the CFREU triggers such supervision by the DPA.

Standard Contractual Clauses, will survive the increased scrutiny elaborated by the CJEU in the *Opinion 1/15*. For example, following the strict standard for *sensitive* data transfers to third countries articulated in *Opinion 1/15,* it is doubtful whether *Privacy Shield* would be found to entail the 'solid justification' for the transfer of sensitive data required by the CJEU in *Opinion 1/15*,[83] Privacy Shield provides that for "…sensitive information.. organisations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected." While the EU Commission has undertaken a first annual review of *Privacy Shield*,[84] it did not address the transfer of *sensitive* personal data, nor identified any "solid justifications" for such transfers in the *Privacy Shield.* Moreover, given the *Privacy Shield* has been criticized for lack of independence of the supervisory authority and the critical view of the CJEU that the proposed PNR Agreement included an 'an authority which does not carry out its tasks with complete independence' (para. 68), the compatibility of the Privacy Shield with EU law is brought into further doubt following the *Opinion 1–15.*

Moreover, the legality of another data transfer mechanism, the *Standard Contractual Clauses* are currently being challenged in *Schrems II* case before the Irish High Court, which has already referred the case to the CJEU on 4th October 2017. The *Standard Contractual Clauses* are relied on by 88 per cent of EU companies transferring data outside the EU, the implications of *Schrems II* potentially may be even more significant than with the fall of *Safe Harbor* after *Schrems.*

So Will Anything Really Change?

Following Snowden revelations, the Court has been very vocal on the constitutional significance of data protection in EU legal framework, and in *Opinion 1/15* it has once again asserted the fundamental role of the protection of personal data in the EU legal order and transatlantic relations. Many other international agreements and adequacy decisions of the EU could be vulnerable to the strict data protection standards applied in *Opinion 1/15.* While they are vulnerable, *Opinion 1–15* does not mean that *Privacy Shield* or PNR regimes are in any immediate jeopardy.

Surely, *normatively speaking,* the EU Commission may – and should - amend the PNR agreements with the US and Australia, as well as the *Privacy Shield* to take account of the issues raised by the CJEU in *Opinion 1–15*. However, different institutions of the EU often maintain distinct strategic priorities that might be difficult to reconcile. The differences between the judicature and executive branches of the EU that evolved in the recent history of transatlantic data-sharing cooperation thus should not be undermined in evaluating the implications of the Opinion 1-15. In the light of recent political and legal pronouncements in the aftermath of the *Schrems* case, it remains doubtful whether the CJEU's insights will be taken seriously by the EU Commission and Council of EU in the future EU negotiations of data sharing agreements with third countries and international organizations.

Indeed, it was initially anticipated that the sweeping nature of the *Schrems* decision could have implications not only for *Safe Harbour*, but also for other US-EU data-sharing arrangements, especially in the law enforcement field, including the PNR, SWIFT and the new *Umbrella*

---

83 Opinion 1/15, para. 165.

84 *Report From The Commission To The European Parliament And The Council on the first annual review of the functioning of the EU–U.S. Privacy Shield,* Brussels, 18.10.2017 (COM(2017) 611).

Agreement.[85] On the one hand, the ruling in *Opinion 1/15* might indeed be considered such an indirect implication, leading the CJEU to consolidate high data privacy standards in the post-Snowden era. Remarkably the CJEU took an unprecedented step and explicitly extended its jurisprudential principles elaborated in post-Snowden case-law to EU external relations. By doing so, the Court reinforced the narrative that EU data protection standards must be affirmed on a global scale.[86] On the other hand, however, even the *Privacy Shield* seems to have changed little on the other side of the Atlantic. While the CJEU took leadership in *Schrems*, and, as some put it, had guts to 'fight back against the NSA',[87] the executive branch of the EU still demonstrated its unwillingness to even attempt to engage in a serious political negotiation. Apparently, demands for a genuine commitment to stop bulk collection of personal data 'was a political bridge too far.'[88] In this sense, some commentators are right to claim that the EU Parliament and CJEU - who have adopted a stronger data privacy stance than the EU Commission and Council - are unlikely to see the desired reforms in US intelligence practices with the *Privacy Shield* in place.[89]

Surely, the CJEU could respond, like in *Schrems*, by invalidating the *Privacy Shield* or PNR agreements with US and Australia, but *Opinion 1/15* - which did not question the very necessity of the PNR agreements - could also signal that the CJEU may have now accepted that the threats to suspend data transfers to the US as leverage to renegotiate for increased data protection standards have not been very effective on political level to this date.[90] So while the CJEU insisted on some fundamental reforms in *Schrems*, the EU Commission has effectively denied such a course of action by simply engaging in a 'cosmetic' make-over of *Safe Harbour* agreement into what became the Privacy Shield. Even though under the new arrangement, the US has promised to respect the CJEU's desire for a high level of data protection.[91] However, it is unlikely to honour that promise.[92] The EU, in turn, is far too economically interdependent with the US to seriously consider suspending data transfers,[93] and will likely have no choice but to ignore breaches of *Privacy Shield* for the sake of economic stability. It may be prepared to be tougher with Canada and Australia but even then it is unlikely to want to block transfers indefinitely.

Some scholars, such as Joel Reidenberg thus argue that lacking an international legally binding agreement on data privacy, the EU institutions will have to accept that its standards will not be enacted on a global degree and especially as far as the US is concerned.[94] The aftermath of

---

85 Weiss, Martin A., and Kristin Archick. *US-EU Data Privacy: from Safe Harbor to Privacy Shield*. Congressional Research Service, 2016, p. 15.

86 See Vedaschi, Arianna. "Privacy and data protection versus national security in transnational flights: the EU–Canada PNR agreement." *International Data Privacy Law* (2018), Vol 8, (advance access), p. 15

87 Farrel and Newman, *Transatlantic Data War*.

88 Gert Vermeulen, 'The Paper Shield: On the degree of protection of the EU-US privacy shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services' in Svantesson, Dan J.B. and Dariusz Kloza (eds.) (2017) *Transatlantic Data Privacy Relationships as a Challenge for Democracy*; Intersentia, Cambridge, at p. 6.

89 Kuner, Christopher. "Reality and illusion in EU data transfer regulation post Schrems." *German LJ* 18 (2017): 881, p. 4.

90 Kuner, *Reality and Illusion*, pp. 19–20; Weiss and Archick, *US-EU Data Privacy*, p. 12, see also Tzanou, Maria. "European Union regulation of transatlantic data transfers and online surveillance." *Human Rights Law Review* (2017),

91 Kuner, *Reality and Illusion*, pp. 20–23.

92 Weiss and Archick, *US-EU Data Privacy*, p. 12; Kuner, *Reality and Illusion*, p. 20.

93 Weiss and Archick, *US-EU Data Privacy*, p. 8 (discussing the European Commission's three broad priorities for ensuring that EU-US data transfers occur while Safe Harbor is re-negotiated).

94 Joel R. Reidenberg, The Transparent Citizen, 47 *LOY.U.CHI. L.J.* 437, 462 (2015).

Schrems case casts doubt whether the EU can compromise with the US standards without surrender in the international data privacy game.

On the other hand, the EU institutions have been further energized by the coming into force of the GDPR as well as the recent Cambridge Analytica revelations, which spurred worldwide debates about the normative implications of collecting and processing personal data. The GDPR and Cambridge Analytica scandal represent yet another milestone in transatlantic data privacy relations, which could provide the CJEU with another opportunity to exert yet even more pressure on the EU Commission and Members States. The Court will soon have a chance to do so and clarify whether data privacy requirements established in *Digital Rights Ireland* and *Tele 2 Sverige* apply in the context of national security. This opportunity follows from the Request for Preliminary Ruling made by the UK Investigatory Powers Tribunal on 18 October 2017, following a series of legal challenges to the national surveillance framework in the UK brought by Privacy International.[95] In this ruling, the CJEU will thus clarify whether limitations to data protection rules in the context of national security remain the sole responsibility of EU Member States under Article 4 TFEU, or whether they are now subject to EU law and scrutiny of the CJEU.[96] However, having in mind relatively limited political effects of the *Schrems* case – which was widely celebrated as another victory for fundamental rights against international surveillance[97] – it is doubtful whether the CJEU pronouncement in *Opinion 1/15* will have enough force in changing the *status quo* in international data privacy game.

CONCLUSION

Opinion 1/15 presented the CJEU with an unmissable opportunity to create a solid precedent on data protection and international agreements. The Court indeed did not miss that chance, and *Opinion 1/15* adds yet another layer to an increasing data privacy constitutionalisation in the EU legal order, while at the same time further contributing the escalating data privacy tensions internationally. This note has argued that the real significance of the *Opinion 1/15* can only be appreciated in a broader historical context of an increasing securitization on the international level since 09/11, which has dominated transatlantic privacy relations until the Snowden revelations. It has employed historical institutionalist analysis to show that *Opinion 1/15* emerges as a powerful addition to the existing data privacy trilogy established by the CJEU in the post-Snowden era in an attempt to re-balance the terms of international cooperation in data-sharing by the EU and other countries. These terms were largely modelled around national security interests that have gained significant prominence in the aftermath of the 9/11 events. While the pro-securitization policies have indeed been very successful in gaining prominence among different private and public actors, e.g., in handling passenger name records (PNR) or personal data in financial transfers (SWIFT), it is however questionable whether CJEU's pushback – without the support of EU Commission or Member States - will receive similar success on international level any time soon.

---

95 See the website of the UK Investigatory Powers Tribunal, http://www.ipt-uk.com/judgments.asp?id1⁄441.

96 For a discussion, see Kuner, Christopher, *et al*. "An unstoppable force and an immoveable object? EU data protection law and national security." (2018) *International Data Privacy Law*, Vol.8, No 1, pp. 1-3.

97 Tzanou, *European Union regulation of transatlantic data transfers and online surveillance.* p.2.