ARTICLES

The Novelty of EU Passenger Name Records (PNR) in EU Trade Agreements: On Shifting Uses of Data Governance in Light of the EU-UK Trade and Cooperation Agreement PNR Provisions

Elaine Fahey*, Elspeth Guild** and Elif Kuskonmaz***

ABSTRACT: The EU-UK Trade and Cooperation Agreement (TCA) offers a new chapter in the treatment of Passenger Name Records (PNR), placing PNR law in an EU trade agreement. The TCA exemplifies acutely pre-existing tensions now in the framework of an EU agreement with a third country. In this *Article*, we examine the evolution of PNR law and look at aspects of the TCA as to PNR relating to the sensitive issue of personal data protection in the context of cross-border data sharing for law enforcement, criminal justice, and border control purposes as an example of the thorny intersection of public law obligations placed on the private sector to provide bulk access to personal data collected for commercial purposes to public sector actors in the framework of counter-terrorism or countering serious crime. First, we provide a brief account of 'repurposing' the use of PNR data at the intersection of criminal justice and border controls in EU law and UK law. Secondly, we examine the question of oversight in EU law and under the TCA. Thirdly, we consider the TCA provisions on PNR data sharing in light of the strict fundamental rights review that the CJEU has adopted. Finally, we look at the incorporation of PNR data sharing into the agreement's law enforcement section and the character of border control and criminal justice. The *Article* argues that PNR law appears vulnerable when seen in the light of the other international data transfers emerging on the question of oversight and accountability.

KEYWORDS: Passenger Name Records – UK-EU relations – trade and cooperation agreement – data adequacy – governance – CJEU.

* Professor of Law, City University of London, elaine.fahey.1@city.ac.uk.
** Professor of Law, Queen Mary University of London, e.guild@qmul.ac.uk.
*** Lecturer in Law, University of Essex, e.m.kuskonmaz@essex.ac.uk.

EUROPEAN PAPERS
VOL. 8, 2023, NO 1, PP. 273-299
www.europeanpapers.eu
ISSN 2499-8249
doi: 10.15166/2499-8249/651

I. Introduction

The international transfer of personal data from the European Union (EU) to third countries constitutes a minefield. It engages multiple national constitutional protections, EU data protection rights and international law – and increasingly, now more recently, trade law. Differing approaches and standards of personal data protection in different States and regions have resulted in stalemates between States or groups of States on the transfer of such data. The political struggles thus have emerged over data sharing, resulting in attempts to regulate how and why the data should be made available to various state agencies and commercial actors.[1]

Nowhere is this political struggle more flagrant and sensitive than in the area of air transport, with different actors (e.g., commercial airlines, border authorities, law enforcement authorities, and security agencies) having interests in the production and sharing of data. In the post-9/11/2001 era, the United States (US) demanded advanced access to as much information as possible about people travelling to the US for counter-terrorism purposes. The US insistence on access to personal data triggered a saga of data politics which is far from over.[2] Passenger Name Records (PNR) are the terrain where this data politics is taking place. PNR is made up of numerous elements of personal data provided by passengers when seeking to book travel but unverified by either the private sector to which they are provided by the data subject or the public sector, which requires the private sector to transmit them on request. The inherent relationship of PNR data with the crossing of international border is a complex one already. Brexit, which moved the United Kingdom (UK) from the status of an EU State to a third country (in EU legal parlance) and the treatment of PNR post-Brexit, has put a novel spotlight on this area of law, illuminating the tremendous complexity and political salience of the legal discord.

[1] Y Soda, *The Politics of Data Transfer* (Routledge 2017); C Fanny, 'The Legitimacy of Bulk Transfers of PNR Data to Law Enforcement Authorities under the Strict Scrutiny of AG Mengozzi' (2016) European Data Protection Law Review 596; S Roda, 'Shortcomings of the Passenger Name Record Directive in Light of Opinion 1/15 of the Court of Justice of the European Union' (2020) European Data Protection Law Review 66; P de Hert and B de Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift' in B Martenczuk and S van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations* (VUB Press 2008); H Carrapico, A Niehuss and C Berthélémy, 'Sectoral Views on Brexit and Future UK-EU Internal Security Relations' in H Carrapico, A Niehuss and C Berthélémy, *Brexit and Internal Security* (Palgrave 2019); N Ni Loideain, 'Brexit, Data Adequacy, and the EU Law Enforcement Directive' in E Kosta and F Boehm (eds), *The Law Enforcement Directive: A Commentary* (OUP 2023); D Korff, 'EU Fundamental Rights Agency: "Thematic Study on Assessment of Data Protection Measures and Relevant Institutions" – Country Report on the United Kingdom' (15 February 2009) SSRN Paper ssrn.com; O Garner, 'Part Three of the EU-UK TCA – From a "Disrupted" Area of Freedom, Security and Justice to "New Old" Intergovernmentalism in Justice and Home Affairs?' (Brexit Institute Working Paper Series 1-2021).

[2] Data politics is coined as the framework to analyse "how data is generative of new forms of power relations and politics at different and interconnected scales". D Bigo, E Isin and E Ruppert, *Data Politics: Worlds, Subjects* (Routledge 2019) 4.

The novelty of the post-Brexit arrangement for the EU-UK PNR data sharing is its placement within a *trade* agreement, the highly esoteric EU-UK Trade and Cooperation Agreement (TCA). This *Article* argues that its provisions require a re-evaluation of this data sharing for they potentially fall short of fundamental rights standards required by EU law. This is not to say that the sharing and processing of PNR data for security purposes have not been contested before Brexit. At the level of the EU, there has long been a mistrust of the capacity of the EU to evolve PNR law in a manner consistent with or compatible with the scope of EU law and the rule of law principles. This mistrust initially materialised in the issues concerning the transfer of PNR data to third countries with an earlier judicial interpretation of the EU competence to legislate that transfer, followed by an exceedingly complex threshold for PNR data transfer arrangements in light of the Charter rights to privacy and personal data protection.[3] The PNR provisions of the TCA must now meet that threshold for the UK to continue to receive PNR data from EU-based commercial airline operators. However, the PNR regulation, including the purposes of the data processing, actors involved in the implementation of regulatory rules as well as the role of the data for law enforcement cooperation, continues to evolve under EU law as the EU PNR Directive, which is the EU secondary legislation on processing PNR data for counter-terrorism and serious crime purposes, is subject of strategic litigation before the Court of Justice of the European Union (CJEU). The first of the series of strategic litigation came to fruition with the CJEU's July 2022 decision of *Ligue des droits humains*.[4] The judicial outcome was a Charter-compliant reading of the EU PNR Directive, with highly significant impacts on the regulation of PNR processing for security purposes in a more institutionalised and rights-based framework. These judicial developments require a constant reconsideration of PNR data sharing arrangements.

The TCA offers a new chapter in this domain, exemplifying the existing tensions in the framework of an EU agreement with a third country, albeit in the context of a trade agreement. It redefines data processing purposes to find mutual ground for the use of PNR data under UK law on the one hand and the outcomes of the judicial review of PNR data transfers and schemes under EU law on the other. The final product, as materialised

[3] Case C-317/04 *Parliament v Council* ECLI:EU:C:2006:346; Opinion 1/15 *Draft agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data* ECLI:EU:C:2016:656.

[4] Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:49. There were other preliminary rulings requests which were all terminated following an enquiry by the CJEU asking whether the referring court wishes to maintain the proceedings in the light of the judgement in Case C-817/19. All referring courts responded that they would not wish to continue the proceedings. See, respectively, Case C-486/20 Request for a preliminary ruling from the Ustavno sodišče Republike Slovenije (Slovenia) lodged on 1 October 2020 – *Varuh človekovih pravic Republike Slovenije* ECLI:EU:C:2022:766; Case C-215/20: Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 19 May 2020 – *JV v Bundesrepublik Deutschland* ECLI:EU:C:2022:773; Case C-222/20 Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 27 May 2020 – *OC v Bundesrepublik Deutschland* ECLI:EU:C:2022:773; Cases C-148/20, C-149/20 and C-150/20 Requests for a preliminary ruling from the Amtsgericht Köln (Germany) lodged on 17 March 2020 – *BD v Deutsche Lufthansa AG*.

in the PNR provisions of the TCA, raises questions on its compatibility with EU law requirements based on three points: the lack of clarity as regards the authority responsible for the correct implementation of the PNR processing rules, the "adequacy" of the protection afforded to PNR data under the TCA, and the coherence of PNR data transfers as enshrined in the TCA with the criminal law cooperation.

Based on the above issues, in this *Article*, we descriptively examine the evolution of PNR law, with a focus on the TCA. We consider aspects of the TCA which play a critical role in the success or failure of the new relationship on data sharing after Brexit. For this reason, first, we provide a brief account of repurposing the use of PNR data at the intersection of criminal justice and border controls in EU law and UK law to introduce different actors with interests in the production and sharing of data and the attempts to designate an appropriate normative framework to govern these activities. Secondly, we examine the question of oversight in EU law and under the TCA because the agreement is sprinkled generously with provisions for oversight on account of the TCA's efforts to implement Opinion 1/15, where the CJEU struck down the EU-Canada PNR agreement as to its oversight provisions.[5] Yet the robustness of oversight leaves questions as to the capacity of the system to fulfil EU and ECHR requirements of independence and effectiveness. Thirdly, we consider the TCA's two provisions that concern the repurposing of PNR data processing in light of the CJEU's strict fundamental rights. Finally, we look at the incorporation of PNR data sharing into the agreement's law enforcement section and the robustness of that framework in the TCA. Based on these four issues, the *Article* argues that PNR law, even post-Opinion 1/15 and *Ligue des droit humains* appears vulnerable when seen in the light of the other international data transfers emerging in *Schrems I* and *Schrems II* on the question of oversight and accountability. These vulnerabilities are argued to be exemplified well in the EU-UK PNR provisions of the TCA and UK-EU adequacy decision.

All these aspects relate to the sensitive issue of personal data protection in the context of cross-border data sharing for law enforcement, criminal justice, and border control purposes. We take the case of PNR as a paradigmatic of data politics arising under the agreement for several reasons. PNR data sharing is argued here to be a clear example of the intersection of public law obligations placed on the private sector to provide bulk access to personal data collected for commercial purposes to public sector actors in the framework of counter-terrorism or countering serious crime. PNR data collection and sharing regimes uncover complex assemblages of parties interested in the production and mobilisation of data with a knock-on effect on legal regulation. It also raises questions about cross-border data protection not only of aliens (or third-country nationals as regards the EU) but also citizens of the state participating in the data sharing operation. These questions require rethinking who can claim rights for such operations and the position of citizens *vis-à-vis* the State. Our focus in this *Article* is exclusively on the EU dimension of PNR and the implications of the TCA provisions.

[5] Opinion 1/15 cit.

II. From its commercial origin to the acquired purpose: the shifts of PNR data

The story of how public actors have become interested in using Passenger Name Records (PNR) in the border security context reveals not only the repurposing of a type of information used by the private sector but also an effort to find a normative legal base for this repurposing through enacting national laws with extraterritorial effects and brokering international agreements to solve conflicts of laws.[6] In this quest, the actors involved in shaping the legal landscape for regulating the use of PNR data have varied, and the purpose of this use has been reshaped into one of ensuring security. For this reason, to analyse how the provisions of the EU-UK Trade and Cooperation Agreement (TCA)[7] govern the sharing of PNR data and the questions of legitimacy and accountability arising from them, it is important to shed light on this process of recasting the use of PNR data at the juxtaposition of criminal justice and border control tools.

A key point which emerges from the origins of PNR data is that this type of data had been created by the private sector for its use in the commercial air travel sector. As the civil aviation sector has grown, it has become essential to keep track of information relating to air travel. In addition to the main information air carriers were asked to collect about their passengers[8], the sector started to collect different types of information such as ticket payment forms, travel agent, the person making the reservation, and in-flight meals if requested.[9] All this information is contained under a generic term, PNR, collected by or on behalf of air carriers each time a passenger books a flight. Since PNR data was originally introduced in the civil aviation sector, there has not been a unified form according to which the data ought to be collected by private actors such as airline operators, computer reservation systems, global distribution systems, and travel agencies.[10]

The 1990s witnessed the use of PNR data, particularly by the US, in border control action based on voluntary cooperation by air carriers.[11] As the 9/11/2001 attacks led to the revamping of security-led policies, policies relating to border controls were similarly

[6] E Guild and E Brouwer, 'The Political Life of Data: The ECJ Decision on the PNR Agreement between the EU and the US' (26 July 2006) CEPS www.ceps.eu.

[7] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part ST/5198/2021/INIT (EU-UK TCA) [2021].

[8] Art. 29 of the Chicago Convention (Convention on International Civil Aviation, ICAO Doc 7300 (1944)) requires every aircraft engaged in international navigation to carry certain documents, including, a list of passengers' names and places of embarkation and destination.

[9] International Civil Aviation Organisation (ICAO), Guidelines on Passenger Name Record (PNR) Data, Doc 9944 (2010), www.icao.int.

[10] PP Belobaba, C Barnhart and WS Swelbar, 'Information Technology in Airline Operations, Distribution and Passenger Processing' in P Belobaba, A Odoni and C Barnhart (eds), *The Global Airline Industry* (Wiley 2016).

[11] For discussions on the passenger profiling in the US before the 9/11 events see E Baker, 'Flying While Arab – Racial Profiling and Air Travel Security' (2002) Journal of Air Law and Commerce 1375.

affected.[12] The emphasis was placed on the pre-emptive actions that were operationalised through increased data mining and profiling.[13] First, the US enacted legislation with the extraterritorial effect which obliges air carriers to share PNR data with the then-newly established US border control authority, the Department of Homeland Security (DHS), if they operate flights to or over the US to ensure the unhampered access to the data by the DHS.[14] The regulatory differences on data protection in the other jurisdictions where operators are based may have been overlooked because the consequence of this legislation was a conflict of laws with EU data protection law that has resulted in the need for a series of agreements on PNR data sharing, with the US and Canada most notoriously. This US legislation and the consequent negotiations to settle the conflict of laws with the EU have influenced many other jurisdictions, and the requests by public authorities to gain routine access to PNR data have spread like wildfire.[15] Thus efforts to collect and repurpose PNR data are not jurisdiction specific.

In the UK, the use of PNR data followed post-9/11/2001 initiatives of the US. The digitalisation of border controls to "create a joined-up modernised intelligence-led border control and security framework" involved the repurposing of PNR data in UK law to this aim.[16] The Immigration, Asylum and Nationality Act 2006 provides specific powers for immigration authorities and police to obtain PNR data from air carriers and share it with public authorities.[17] Thus, repurposing PNR data had been an inherent part of the UK border control, which involved law enforcement functions as well. Reading the PNR data use within this frame will be significant for our discussion in Section V on whether PNR systems are captured solely by a criminal justice or border control framework.

The EU was not immune from the post-9/11/2001 initiatives of repurposing PNR data. It began working on creating its own PNR scheme in 2004.[18] By the time the EU was progressing towards legislating for harmonised rules governing the use of PNR data for

[12] V Mitsilegas, 'Extraterritorial Immigration Control in the 21st Century: The Individual and the State Transformed' in B Ryan and V Mitsilegas (eds), *Extraterritorial Immigration Control* (Brill 2010).

[13] M de Goede, 'The Politics of Privacy in the Age of Preemptive Security' (2014) International Political Sociology 100.

[14] Aviation and Transportation Security Act of 2001 of United States, 49 USC *§* 44909.

[15] See, for example, Security Council, Resolution 2396 of 21 December 2017, UN Doc S/Res/2396 (2017). See also O Mironenko Enerstvedt, 'Russian PNR System: Data Protection Issues and Global Prospects' (2014) Computer Law & Security Review 25; K Taplin, 'South Africa's PNR Regime: Privacy and Data Protection' (2021) Computer Law & Security Review 105524.

[16] Home Office, *Controlling our Borders: Making Migration Work for Britain – Five Year Strategy for Asylum and Immigration* assets.publishing.service.gov.uk.

[17] Immigration, Asylum and Nationality Act 2006, ss 32-38. The types of information to be shared and the requirements for this sharing were laid out in secondary legislation. See The Immigration and Police (Passenger, Crew and Service Information) Order 2008 (United Kingdom), Schedules 1-4.

[18] E Fahey, 'Of "One Shootters" and "Repeat Hitters": A Retrospective on the Role of the European Parliament in the EU-US PNR Litigation' in F Nicola and B Davies (eds), *EU Law Stories: Contextual and Critical Histories of European Jurisprudence* (CUP 2017).

counter-terrorism and countering serious crime, the UK had already set up its own PNR system.[19] Yet, in 2011, it still chose to opt-in to the (then draft) EU PNR Directive.[20] Following a tumultuous decade of back-and-forth,[21] the EU PNR Directive was adopted in 2016.[22] The Directive was implemented in UK law,[23] but the UK's participation in the EU PNR scheme was jeopardised by Brexit.

The latest settlement or solution, one which is unique for its location in a trade agreement, to enable PNR data sharing from the EU to the UK is found in the EU-UK TCA. However, the robustness of this solution can be contested, starting from the appropriateness of the checks and balances that it introduces to ensure fundamental rights compliance. To address this legal debate, the next section turns to the question of oversight as a key legal issue of its legality post-Opinion 1/15.

III. The EU-UK TCA and the problem of oversight in EU PNR law

III.1. The EU-UK TCA PNR provisions

Title III of the TCA makes provision in approximately 20 articles for PNR law. The transfer of PNR thus is provided for in Part III, Title 3, TCA. It is unusually detailed and comprehensive in a trade agreement.[24] Oversight is not, however, a separate dedicated article of the TCA. It is mentioned once in one article, art. 554, on the logging and documentation of PNR data processing by the competent authority – which has to "ensure oversight" in para. d) thereof.[25]

Many entities are provided for in the TCA to be involved in governance, supervision, communication, transfer, review, and accountability. They arguably inform its oversight cumulatively. These include in Part III a Competent Authority, Passenger Information Units (PIU), Specialised Committee on Law Enforcement and Judicial Cooperation (Specialised Committee), independent reviews, judicial review and a Partnership Council. This

[19] House of Lords, European Union Committee, *The United Kingdom opt-in to the Passenger Name Record Directive* (HL 2010-11 113) publications.parliament.uk.

[20] Communication COM(2011) 32 final from the Commission of 2 February 2011 on 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.

[21] M Nino, 'The Protection of Personal Data in the Fight Against Terrorism: New Perspectives of PNR European Union Instruments in the Light of the Treaty of Lisbon' (2010) Utrecht Law Review 62.

[22] Directive 2016/681/EU 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.

[23] See section III below.

[24] E Cummins, 'The UK-EU Trade and Co-operation Agreement 2020' (18 January 2021) Senior European Experts senioreuropeanexperts.org.

[25] Art. 554 of EU-UK TCA cit.

is in addition to the broader governance structure of the TCA.[26] In total, it appears that there are at least 5 layers of oversight.

The concept of "*competent authority*" is thus defined in art. 543 of the TCA and is pivotal to the operation of PNR here. It refers to the UK authority responsible for receiving and processing PNR data under the TCA. This competent authority is what the PIUs are for the Member States.[27] The TCA and PIUs, in turn must "cooperate" with one another, which provides a rare instance of bilateral institutional cooperation provided for under the TCA.

The main powers to use PNR data of the competent authority are set out in art. 544(2) on the purposes of the use of PNR data.[28] Art. 552(3) on retention of PNR data finally provides for unmasking powers in a limited number of scenarios.

The competent authority entity or concept is to be distinguished from the "*independent administrative body*", as referred to in arts 552(7), 552(11)(d), 552(12)(a) and 553 since this body has explicitly to be independent from the UK competent authority (UK PIU). This independence is necessary to "assess on a yearly basis the approach applied by the [UK] competent authority as regards the need to retain PNR data pursuant to paragraph 4".[29] It is also the only entity expressly mandated to ensure "oversight" in relation to PNR data pursuant to art. 554.[30] It thus, on its face, complies with the CJEU's Opinion 1/15.[31] The independent authority is required to supervise compliance with and enforcement of data protection. Thus, it is a key actor of change in the TCA, marking a shift away from the EU-Canada PNR Agreement, where such oversight was not provided for.[32]

Art. 546(1)-(4) provides that the UK competent authority shall share data "upwards" and "horizontally" with Europol or Eurojust or horizontally with the PIUs of the Member States as soon as possible in specific cases where necessary to prevent, detect, investi-

[26] N Levrat, 'Governance: Managing Bilateral Relations' in F Fabbrini (ed), *The Law & Politics of Brexit* (vol. 3 OUP 2021).

[27] In the UK this is the Home Office (National Border Targeting Centre Independent Compliance Governance Team).

[28] It provides that: "In exceptional cases, the [UK] competent authority may process PNR data where necessary to protect the vital interests of any natural person, such as (a) risk of death or serious injury; or (b) a significant public health risk, in particular as identified under internationally recognised standards."

[29] Art. 552(7) of EU-UK TCA cit.

[30] Art. 554 of EU-UK TCA cit.

[31] Opinion 1/15 cit. paras 228-231.

[32] This follows not only from the TCA but also from art. 36 of the Law Enforcement Directive (LED) as it requires the EU to monitor the compliance of the data protection conditions by third countries, including a periodic review to reassess the adequacy decision (see art. 36 of Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED)).

gate, or prosecute terrorism or serious crime. However, pursuant to para. 6, the UK competent authority and the PIUs of the Member States are required to ensure that only the minimum amount of PNR data necessary is shared under paras 1 to 4.[33]

Beyond these bodies sits a *Specialised Committee on Law Enforcement and Judicial Cooperation*. Art. 525(3) of the TCA provides that the Specialised Committee will be responsible for overseeing the data protection rules applicable to the cooperation under Part III.[34] It thus establishes a Committee to assist the Parties in their endeavour to reach a consensual solution and to foster their cooperation when allegations of breach of their duties under the TCA arise. However, the dispute settlement mechanism under Part III of the TCA does not refer to a standing judicial body or the establishment of panels.

It has powers to take reports and thus provides for reporting and accountability in art. 552(12) of the TCA, and importantly, the UK must provide a report for the independent administrative body.[35] Thus, art. 549(4) of the TCA develops the next layer of oversight: it provides that "[t]he [UK] competent authority shall promptly inform the Specialised Committee on Law Enforcement and Judicial Cooperation of any significant incident of accidental, unlawful or unauthorised access, processing or loss of PNR data".[36]

Opinion 1/15 found that oversight entailed that PNR titles had to be "subject to prior review either by a court or by an independent administrative body".[37] The terms "*court or independent administrative body*" were mentioned in art. 552(7) refer to and on its face comply with the requirements set out by the CJEU in its Opinion 1/15 on the use and disclosure of PNR. However, courts play a role in only 2 instances – arts 553 and 544 reference the capacity of a court to conduct a prior review or compel oversight. Art. 552(7), in conjunction with art. 552(12) (a) also provides that the [UK] shall ensure that a domestic supervisory authority responsible for data protection will have the power to supervise compliance with and enforcement of data protection. On its face, these operate as a series of multiple governances and accountability checks – cumulatively *layers* of oversight.

In addition to all the above, the TCA establishes the *Partnership Council* – chaired by both the UK and EU – at the apex thereof to oversee the implementation, application, and

[33] Art. 546(6) of EU-UK TCA cit.

[34] Art. 525(3) of EU-UK TCA cit.

[35] The provision further specifies that the report "[…] shall include the opinion of the [UK] supervisory authority referred to in Article 525(3) as to whether the safeguards provided for in paragraph 11 of this Article have been effectively applied"; the UK shall also provide to the Specialised Committee on Law Enforcement and Judicial Cooperation "the assessment of the [UK] of whether the special circumstances referred to in paragraph 10 of [Article 552] persist together with a description of the efforts made to transform the PNR processing systems of the [UK] into systems which would enable PNR data to be deleted in accordance with paragraph 4 of [Article 552]". See art. 552 (12) (a) and (b), respectively, of EU-UK TCA cit.

[36] Art. 549(4) of EU-UK TCA cit. See A Janet, 'Dispute Settlement and Jurisdictional Issues for Law Enforcement and Judicial Cooperation in Criminal Matters under the EU–UK Trade and Cooperation Agreement' (2021) New Journal of European Criminal Law 290.

[37] Opinion 1/15 cit. para. 208.

interpretation of the TCA in Title III, art. 7.[38] The function of the Partnership Council becomes significant directly and indirectly to oversight issues. For instance, the PNR data of most travellers have to be deleted after their stay in the UK has ended, which is an important development in line with Opinion 1/15.[39] However, for example, the UK did not have to apply this provision in 2021 and 2022 because of a derogation – one that could be extended for another year if the Partnership Council agreed to it pursuant to art. 552(13).

III.2. Operation of the TCA oversight provisions in practice

PNR data of travellers that are not suspected of crimes and whose information is not needed for law enforcement purposes could be kept by the UK for another two years before the deletion obligation comes into force because of the operation of a Council decision, and the Partnership Council decision.[40] It has been argued that the EU should not be tied by any arbitrary deadline and consider the overall protection of data being transferred at every opportunity.[41] However, early in the relationship, this decision was taken with swift application. The first meeting of the Specialised Committee on Law Enforcement and Judicial Cooperation took place on 19 October 2021, with minutes published only several months later, where pursuant to art. 552, considered the UK report and assessment of Passenger Name Record Data. They noted that the opinion of the UK supervisory authority included with the report of the independent administrative body (IAB) provided under art. 552(12) of the TCA was based only on the information contained in the report of the IAB. The UK indicated that in view of the unique situation arising as a result of COVID-19 the UK supervisory authority was prepared to provide a note to complement its opinion in November following a review of the operation of the interim period safeguards undertaken directly by the UK supervisory authority.[42] It is difficult to see any legal provision for this "note" or to evaluate its potential legal salience. Then in the second decision of the TCA (Decision 2/2021) Partnership Council, it agreed on a decision on the extension of the interim period on 21 December 2021.[43] The EU

[38] Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community 2019/C 384 I/01 [2019], art. 164.

[39] Art. 552(4) of EU-UK TCA cit.; Opinion 1/15 cit. paras 205-206.

[40] Decision 2021/2293/EU of the Council of 20 December 2021 on the position to be taken on behalf of the Union in the Partnership Council established by the Trade and Cooperation Agreement with the United Kingdom regarding the extension of the derogation from the obligation to delete passenger name record data of passengers after their departure from the United Kingdom.

[41] E Massé, 'Access Now's memo on the data transfers and PNR provisions under the EU-UK Trade Agreement' (2021) Access Now www.accessnow.org.

[42] European Commission, First Specialised Committee on Law Enforcement and Judicial Cooperation under the EU-UK Trade and Cooperation Agreement, 13 January 2022, www.commission.europa.eu.

[43] Decision 2/2021 of the Partnership Council established by the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, of 21 December 2021; Decision 2021/2293/EU cit.; Decision 3/2022 of the Partnership Council established by the Trade and Cooperation

position taken on the Union's behalf in the Partnership Council pursuant to art. 552(13) of the TCA was to agree to extend the interim period during which the United Kingdom may derogate from the obligation to delete the PNR data of passengers after they depart from the United Kingdom by one year, until 31 December 2022. There was scant information available at the time of writing as to how this decision was arrived at nor its implications.

III.3. Analysis

As indicated above, EU PNR agreements with third countries contain variable provisions on oversight, from none to esoteric or non-independent scrutiny.[44] Nor is oversight of PNR law is not also defined explicitly in EU law (or international law), at least until Opinion 1/15. As a result, the *locus* or *place* of PNR, i.e. where it is located as a matter of law, appears worthy of attention as to the place of oversight.[45] Members of the European Parliament individually and *en masse* have for a long time advocated and even litigated for better governance and oversight of PNR.[46] The entire trajectory of EU PNR law has been to add *further* layers of oversight,[47] particular where it is used as alternative to border checks; a point which we will expand on in Section V – arguably warranting more rather than less oversight.[48]

Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, of 21 December 2022 establishing a list of individuals who are willing and able to serve as members of an arbitration tribunal under the Trade and Cooperation Agreement.

[44] E Massé, 'Access Now's Memo on the Data Transfers and PNR Provisions under the EU-UK Trade Agreement' cit.; E Carpanelli and N Lazzerini, 'PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU' (2017) Air and Space Law 377. See also European Commission, *Air travel – sharing passenger name data within the EU and beyond (assessment)*, ec.europa.eu.

[45] E Fahey, 'Of "One Shotters" and "Repeat Hitters": A Retrospective on the Role of the European Parliament in the EU-US PNR Litigation' cit.; E Kuşkonmaz, *Privacy and Border Controls in the Fight against Terrorism* (Brill 2021).

[46] Joined Cases C-317/04 and C-318/04 *European Parliament v Council and Commission* (*PNR Cases)* ECLI:EU:C:2006:346 paras 56-59 and 67-69. See C Docksey, 'The European Court of Justice and the Decade of Surveillance' in H Hijmans and H Kranenborg (eds), *Data Protection Anno 2014: How to Restore Trust?* (Intersentia 2014); Case T-529/09 *In 't Veld v Council* EU:T:2012:215; Opinion 1/15 cit.; M de Goede and M Wesseling, 'Secrecy and Security in Transatlantic Terrorism Finance Tracking' (2017) Journal of European Integration 253.

[47] E Fahey, 'Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program' (2013) Yearbook of European Law 368.

[48] J Jeandesboz, 'Ceci n'est pas un contrôle: PNR Data Processing and the Reshaping of Borderless Travel in the Schengen Area' (2021) European Journal of Migration and Law 431; L Drechsler, 'Setting the Boundaries between the General Data Protection Regulation, the Law Enforcement Directive and the PNR Directive. The Other Important Question Tackled by Advocate General Pitruzzella in Opinion in Case C-817/19 Ligue des droits humains' (11 February 2022) EU Law Live eulawlive.com.

Notably, EU and ECHR laws increasingly appear to have converged initially then somewhat diverged on oversight as to surveillance, with the ECtHR becoming increasingly less strict.[49]

Some contended early on that the provisions in the TCA on PNR contain much of the same content as all existing EU PNR law.[50] Yet this appears untrue in so far as the EU-UK TCA PNR provisions make considerable effort to learn from the provisions of the EU-Canada PNR agreement.[51] In the landmark Opinion 1/15 the CJEU held that the agreement was problematic as to oversight because the oversight was to be carried out, partly or wholly, by an authority which does not carry out its tasks with complete independence.[52] It was, therefore, not free from any external influence liable to affect its decisions.[53] This requirement of independent oversight emerges also as a key theme in *Schrems* II and the place of an independent *Ombudsman* for the EU-US Privacy Shield.[54]

The TCA is much criticised for its broad powers allowing for the transfer of PNR data to the EU.[55] There is no direct effect of the TCA as provided for explicitly therein, with considerable challenges then faced by those seeking to challenge oversight issues.[56] The term "transfer" or "transferred" is ultimately mentioned 32 times in Title III of the TCA. As a result, it can be said that its governance, specifically its oversight, is highly salient still but underwhelming.

[49] V Mitsilegas and others, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2022) ELJ 1.

[50] E Massé, 'Access Now's Memo on the Data Transfers and PNR Provisions under the EU-UK Trade Agreement' cit.

[51] Council of the European Union, Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (Draft Canada PNR Agreement), 12657/5/13 REV 5, 23 June 2014, data.consilium.europa.eu.

[52] Opinion 1/15 cit. para. 230.

[53] C Kuner, 'International Agreements, Data Protection, and EU Fundamental Rights on the International Stage' (2018) CMLRev 857, 868; E Carpanelli and N Lazzerini, 'PNR: Passenger Name Record, Problems Not Resolved?' cit. 386, 388; Zalnieriute, 'Developing a European Standard for International Data Transfers after Snowden' (2018) ModLRev 1046, 1053.

[54] See E Fahey and F Terpan, 'Torn between Institutionalisation and Judicialisation: The Demise of the EU-US Privacy Shield' (2021) IndJGlobalLegalStud 205; and Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559, para. 68.

[55] T Bunyan and C Jones, 'Brexit: Goodbye and Hello: The New EU-UK Security Architecture, Civil Liberties and Democratic Control' (20 January 2022) Statewatch www.statewatch.org. See Regulation 6A of the Passenger Name Record Data and Miscellaneous Amendments Regulations 2018 of the United Kingdom ("the 2018 Regulations of the UK"). The 2018 Regulations of the UK have been amended by the Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 and the European Union (Future Relationship) Act 2020. See also S.7 and Schedule 2, European Union (Future Relationship) Act 2020 of the United Kingdom, www.legislation.gov.uk; European Union (Future Relationship) Act 2020, Explanatory Notes available at www.legislation.gov.uk. See also the Data Protection Act 2018 Schedule 7, Data Protection Act 2018 ("other [competent] authorities" – 52 – ICO).

[56] Art. 5 of EU-UK TCA cit. See European Union (Future Relationship) Act 2020 cit. section 29.

The multitude of actors themselves provides an example of the layers of institutionalised governance emerging, albeit their effectiveness and actual reach of the layers remains to be seen.[57] The main oversight structures of the TCA appear mainly similar to previous PNR Agreements, and it is hard to see the radical change from past practice. Rather, it is an additional later layer of annual reporting that remains the substantive difference, along with the putative layer of courts engaging in judicial review. The extensive range of data transfers taking place unifies academics, civil liberties groups, and NGOs alike.[58] Notably, threats exist on the part of the UK Government post-Brexit to exit the Council of Europe ECHR or overhaul or reform the Human Rights Act operate in the background or "rid" the UK of the GDPR or reform it under the Data Reform Bill as part of the "bonfire" of retained EU law proposed.[59] The effect of such issues remains to be seen for the adequacy decision granted, closely being watched by multiple EU institutions. The opaqueness of the layers of TCA PNR governance will arguably be the most problematic. Ultimately, however, the absence of transparency as to the operation of the oversight provisions overall makes its cumulative impact very difficult to assess. The other problematic aspects of the PNR provisions are the protection of the fundamental rights they offer in terms of the scope of PNR data to be shared with the Home Office.

The next section explores these issues from a more technical perspective, as to "adequacy" explained next.

IV. 'Adequacy' standard for the EU-UK PNR data transfers

IV.1. Overview of 'Adequacy'

Besides being significant in governing the oversight of PNR data transfers, the TCA's PNR provisions set out substantive rules on how data transfers outside the EU should be governed. Because those transfers are carried out seemingly in a law enforcement context, the protection that should be afforded by the TCA to the data bears tremendous significance for the protection of travellers whose data are transferred even though the Agreement is a piece in a patchwork of laws that govern the EU-UK data sharing.

The continuity of PNR data sharing between the EU and the UK after the end of the transition period turned on the observance of international data transfer rules under EU law. At their core, these rules prohibit the transfer of personal data outside the EU unless the recipient country (or the recipient data controller or processor following *Schrems II*)

[57] See N Levrat, 'Governance: Managing Bilateral Relations' cit.

[58] O Garner, 'Part Three of the EU-UK TCA' cit.; T Bunyan and C Jones, 'Brexit: Goodbye and Hello' cit.

[59] UK Government, *The Benefits of Brexit: How the UK is Taking Advantage of Leaving the EU' (January 2022)* www.gov.uk.

affords adequate protection to the data compared to that of EU law.[60] The data sharing arrangements the EU has signed with third countries over the years entails that the recipient country affords an "adequate level of protection" for the transferred data.[61]

Unlike the other PNR data sharing arrangements, the TCA does not declare UK law "adequate" in affording protection to PNR data transferred from the EU. Instead, it sets out certain data protection principles that both parties pledge their allegiances to under art. 522. These principles generally apply to sharing different types of personal data incorporated into the law enforcement section of the TCA. The provisions on PNR data transfers provide rules specific to the sharing of the data by commercial air carrier companies to the UK Home Office (as the "competent authority" described in UK national law and required by the Immigration, Asylum, and Nationality Act 2006), the subsequent processing of the data by the UK Home Office, and the exchanges among the UK Home Office on the one side, and the EU Member States PIUs and the Europol on the other.[62] These rules however must be considered alongside the general data transfer arrangements to the UK.

The answer to retaining data transfers post-Brexit was purely practical. In a separate provision contained outside the law enforcement section, the TCA introduced a bridging period during which data transfers to the UK would not be treated as a transfer to a third country.[63] After the end of this period (which was set to expire on 30 June 2021, including two months extension period), data transfers to the UK would be governed by international data transfer rules under EU law. While this interim solution was provided for the sake of "clarity", especially for the commercial sector, not everyone shared the same optimism for the expected adequacy decisions for commercial data transfers and law enforcement data transfers, not least because the former did not cover the processing for immigration purposes as the question on the legality of UK law that allowed public authorities not to fulfil their obligations concerning data subject rights based on an immigration exemption was still pending.[64]

[60] Ch. V GDPR cit.; ch. V Law Enforcement Directive cit. See also C Kuner, 'Article 44. General Principle for Transfers' in C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Directive (GDPR): A Commentary* (OUP 2020) 764-765; L Drechsler, 'Wanted: LED Adequacy Decisions. How the Absence of any LED Adequacy Decision is Hurting the Protection of Fundamental Rights in a Law Enforcement Context' (2021) International Data Privacy Law 182.

[61] The PNR data-sharing arrangements contain specific adequacy provisions. See art. 5 Draft Canada PNR Agreement cit.; Agreement of 29 September 2011 between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service (EU-Australia PNR Agreement), art. 5; Agreement of 14 December 2011 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 (EU-US PNR Agreement), art. 19.

[62] Arts 542-562 of EU-UK TCA cit.

[63] Art. 782 of EU-UK TCA cit.

[64] Open Rights Group, *The UK's Immigration Exemption in the Data Protection Act 2018 and Data Adequacy*, www.openrightsgroup.org; EDPB, Opinion 15/2021 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data

Despite these concerns, the Commission adopted two separate adequacy decisions almost just in time before the end of the bridging period on 28 June 2021; one relating to commercial data transfers under the General Data Protection Regulation (GDPR)[65] and the other relating to data transfers for law enforcement purposes under the Law Enforcement Directive (LED).[66] Data transfers to the UK are not restricted after this date and can take place based on these two decisions. If the answer to retaining data transfers to the UK lies in these two somewhat controversial adequacy decisions, what is the role of the PNR provisions of the TCA in sustaining the sharing of a particular type of information?

In May 2021, the Parliamentary Research Service attempted to clarify the role of the TCA concerning these adequacy decisions.[67] After the bridging period, the adequacy decision on commercial data transfers provides the basis for PNR data transfers by commercial air carriers to the UK Home Office.[68] According to the TCA, the transfer takes place in connection with law enforcement cooperation and situating it within the scope of adequacy decision based on the GDPR might be puzzling to some. Many scholars have raised more general questions on uncertainties in applying the GPDR and the LED where the private-public partnership is involved in the data processing.[69] In *Ligue des droits humains*, the CJEU addressed several of these uncertainties over the sharing of PNR data from commercial companies to the EU Member States PIUs that are deemed "competent authorities" for LED. In view of the Court, a commercial company was not a competent authority, and thus the data sharing would be covered by the GDPR and not the LED.[70] This means that the more exigent standards of GDPR apply and that any drift away from GDPR standards in the UK

in the United Kingdom, 13 April 2021; EDPB, Opinion 14/2021 Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, 13 April 2021.

[65] 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) 1 ff.

[66] Directive (EU) 2016/680 cit. 89–131. For adequacy decisions, see Communication COM(2021) 4801 final from the Commission implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom; Communication COM(2021) 4800 final from the Commission implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom.

[67] CC Cîrlig, 'Law Enforcement and Judicial Cooperation in Criminal Matters under the EU-UK Trade and Cooperation Agreement' (May 2021) European Parliamentary Research Service www.europarl.europa.eu.

[68] I Hallak and others, 'EU-UK Trade and Cooperation Agreement: An Analytical Overview' (February 2021) European Parliamentary Research Service www.europarl.europa.eu.

[69] MM Caruana, 'The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement' (2019) International Review of Law, Computers & Technology 249; N Purtova, 'Between the GDPR and the Police Directive: Navigating through the Maze of Information in Public-private Partnerships' (2018) International Data Privacy Law 52.

[70] *Ligue des droits humains* cit. paras 67-73.

(as apparent in a bill currently before Parliament)[71] will raise even more questions about the adequacy of the UK data protection system from the perspective of EU law.

The CJEU's above findings seem to confirm that PNR data transfers, at least those by commercial air carrier companies to the UK Home Office, are covered by the UK adequacy decision on commercial data transfers issued under the GDPR.[72] The PNR provisions of the TCA provide additional safeguards to PNR data transfers and the subsequent processing by a "competent public authority", the UK Home Office. As part of an international agreement, these provisions stipulate the transfer and processing of personal data and thus interfere with individuals' right to privacy (art. 7 Charter) and personal data protection (art. 8 Charter). For this reason, the extent to which they successfully provide safeguards to the transferred data and individuals whose data is transferred must be determined based on the EU constitutional framework.[73] The following Sections consider whether the PNR provisions of the TCA are in line with the standard of adequacy based on two issues to highlight the recasting of PNR data use: *i)* the *purpose* for which data may be processed and *ii) procedural* safeguards for access to data.[74]

IV.2. The shifting maze of PNR data processing purposes: from law enforcement to border control

The shift in data transfer purposes is evident in the TCA's PNR data processing provision, which raise questions on the extent to which it satisfies the adequacy standard. Art. 544 of the TCA provided clues in deciphering the oversight mechanism for PNR data sharing in Section III. This article is of significance once again – and this time in determining the

[71] See Data Protection and Digital Information Bill of 2022 bills.parliament.uk.

[72] There is however a question whether PNR data transfers can considered as data transfers for immigration purposes and thus are captured by the exclusion contained in the adequacy decision. The answer lies within how PNR data is used under UK law, which is addressed in Section V.

[73] Opinion 1/15 cit. para. 134.

[74] It is important to note here that the adequacy standard of the PNR provisions of the TCA is one aspect of the complex issues surrounding the continuity of data transfer to the UK. The UK Government has voiced its intention to change UK data protection laws and introduced the Data Protection and Digital Information Bill. Among those areas, the most concerning ones that may indicate a divergence from the current law for which the Commission issued an adequacy decision are the changes relating to the operation of the Information Commissioner's Office, data transfers and the prohibition against automated decision-making. See EDPB, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, 13 April 2021, para. 11; Resolution 2021/2594 of the European Parliament of 21 May 2021 on the adequate protection of personal data by the United Kingdom; A Chromidou, 'EU Data Protection under the TCA: The UK Adequacy Decision and the Twin GDPRs' (2021) International Data Privacy Law 388; N Ni Loideain, 'Brexit, Data Adequacy, and the EU Law Enforcement Directive' cit. These changes may open another can of worms for the suspension or termination of Part 3 of the TCA, but there are multiple routes for either option, and none of them requires an automatic suspension or termination; see S Peers, 'So Close, Yet So Far: The EU/UK Trade and Cooperation Agreement' (2022) CMLRev 49.

purpose for which the Home Office may use PNR data. Accordingly, the data received by the UK can be processed *i*) strictly to prevent, detect, investigate or prosecute terrorism or serious crime; *ii*) to oversee the processing of PNR data within the terms of the TCA;[75] and *iii*) in exceptional cases where necessary to protect the vital interests of any natural person, such as a risk of death or serious injury; or *a significant public health risk*, in particular as identified under internationally recognised standards.[76]

To ensure adequacy, the TCA must prescribe the purposes for which PNR data may be used by the Home Office in a clear and precise manner.[77] Based on the mentioned data processing purposes, two issues emerge: first, how the TCA defines serious crime and second, how it provides data processing for non-crime-related purposes concerning the protection of vital interests of individuals.

On the former issue, the TCA incorporates the definition of serious crime found in the EU PNR Directive by prescribing that a crime is deemed serious if it is punishable by a maximum of three years imprisonment.[78] It does not incorporate a list of serious offences as it does for the definition of terrorist offences contained in Annex 45. This point was criticised by the European Data Protection Supervisor (EDPS) who overall welcomed how the TCA incorporated the CJEU's findings in Opinion 1/15.[79] In *Ligue des droits humains*, the CJEU elaborated further on setting the crime threshold. According to the Court, the seriousness threshold should be based on a maximum penalty instead of a minimum penalty because the latter option would allow the PNR data processing to take place for offences that do not reach the threshold of severity and ultimately result in disproportionate interference with the rights of privacy and data protection.[80] Based on this finding, the definition of serious crime under the TCA might be re-evaluated. More importantly, the CJEU required PNR processing to be permitted not for all serious crimes but only for those with an objective link with air travel.[81] This finding of the CJEU might require reassessing the categories of serious crimes for which PNR data can be processed under the TCA.

The issue with non-crime-related purposes is how they capture processing for protecting individuals' vital interests, *including* public health risks. The EU PNR Directive does not provide processing of PNR data for a public-health-related purpose. As a result, some Member States were concerned that the UK would be supplied with PNR data for a purpose not

[75] Art. 544(1) of EU-UK TCA cit.

[76] Art. 544(2) of EU-UK TCA cit.

[77] Opinion 1/15 cit. para. 154.

[78] Art. 543 of EU-UK TCA cit.

[79] EDPS, Opinion 3/2021 on the Conclusion of the EU and UK Trade Agreement and the EU and UK Exchange of Classified Information Agreement, 22 February 2021.

[80] *Ligue des droits humains* cit. paras 151-152.

[81] *Ibidem.* See also Section IV on the cross-border element of serious crimes.

foreseen in national laws implementing the EU PNR Directive.[82] According to the Commission, however, this provision did not contradict the EU PNR Directive and was in line with Opinion 1/15, where the CJEU was satisfied with the processing of PNR data in exceptional circumstances when public health risks are involved.[83] Based on this finding of the Court, a similar type of data processing contained in the TCA might pass the CJEU's scrutiny.

Regarding UK law, the 2018 Regulations do not explicitly mention the processing of PNR data for health-related purposes, as it does for its rules on processing for terrorism and serious crime-related purposes.[84] But this does not mean that processing PNR data for health-related purposes is prohibited. The 2018 Regulations note that processing of PNR data is required under the UK immigration legislation requiring air carriers (or sea carriers) to provide "information" to an immigration officer.[85] With this, the inherent border control purpose of PNR data sharing that we will sketch in Section V shines through.[86]

In addition to these examples of the shifting of PNR data, the next section considers the conditions for data accessing where we exhibit more evidence for such shifting under the TCA.

IV.3. Conditions to access PNR data

The next question on the adequacy of the PNR provisions of the TCA is how they govern PNR data transfers from commercial air companies and their subsequent access by the UK public authorities. In Opinion 1/15, the transfer of PNR data without an objective link between the travellers whose data are transferred and the so-called security purpose was challenged based on the CJEU's case-law on data retention.

[82] Statewatch, 'Brexit: Commission answers to EU member state questions on the Trade and Cooperation Agreement' (25 January 2021) Statewatch www.statewatch.org.

[83] The Commission also mentioned the interests reported by the Member States to process PNR data for public health purposes although the EU PNR Directive does not envisage such processing purpose; see Communication COM(2020) 305 final from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

[84] The 2018 Regulations of the UK cit. section 5. Annex 45 of the EU-UK TCA defines terrorism. Serious crime is defined by UK law and covers offences punishable for a maximum period of at least three years. The EU-UK TCA does not list conduct that may fall within these categories of offences as the EU PNR Directive does. Still, the CJEU accepted a similar approach in Opinion 1/15, and the definition of serious crime may not raise any issues in regard to legal clarity.

[85] The 2018 Regulations of the UK cit. section 5.

[86] In fact, the UK's interest in requesting PNR data from air carriers for health-related reasons reportedly goes to the 2014 Ebola virus break to screen incoming passengers from the regions that had been affected the most; see M Holehouse, 'David Cameron Says Europe's Block on Sharing Passenger Data Is "Frankly Ridiculous"' (18 December 2014) Telegraph www.telegraph.co.uk.

As a first step, the Court addressed the scope of the draft Canada PNR Agreement that covers PNR data transfer of all passengers in the absence of objective evidence indicating the contribution of the data to the fight against terrorism.[87] The Court thought that this transfer of data *en masse* was within the limits of the strict necessity test and was permissible because, based on this transfer, the Canadian authorities could carry out automated data processing before the arrival of passengers to facilitate and expedite security checks.[88] The objective of ensuring border security could not be achieved by excluding certain categories of people and areas of origin from the scope of PNR data transfers.[89] The Court further noted that the international civil aviation treaty, the Chicago Convention, to which Canada was a signatory party, recognised states' right to prescribe their own national rules on entry and clearance.[90] Pre-emptive border screening enabled through indiscriminate use of PNR data was part of Canada's entry and clearance rules.[91] In its *Ligue des droits humains* decision, the CJEU stood its ground and held that as far as the extra-EU travels are concerned, the legislation does not have to condition PNR data transfers on the existence of objective evidence that the data transfer would contribute to the fight against terrorism and serious crime.[92]

Based on the CJEU's above findings, the *adequacy* standard of the PNR provisions of the TCA would not be affected by the absence of objective evidence.[93] However, the CJEU notes that once the data is used in pre-screening procedures, its subsequent access by public authorities must be subject to further procedural safeguards because the purpose of the processing ceases to exist once the person is admitted into or departs from the country.[94] For this purpose, systematic access to the retained data is prohibited.[95] The legislation thus must define circumstances and conditions based on objective criteria allowing authorities access to the retained data.[96]

At its face value, the TCA follows the adequacy requirements laid out by the CJEU to an extent. Accordingly, the Home Office may use PNR data for purposes "*other than security and border control checks*", where "new circumstances based on objective grounds indicate

[87] Opinion 1/15 cit. para. 186.

[88] *Ibid.* para. 187.

[89] *Ibid.* para. 187.

[90] *Ibid.* para. 188.

[91] *Ibid*.

[92] *Ligue des droits humains* cit. paras 161-162.

[93] Art. 542 of EU-UK TCA cit.: "2. This Title applies to air carriers operating passenger flights between the Union and the United Kingdom. 3. This Title also applies to air carriers incorporated, or storing data, in the Union and operating passenger flights to or from the United Kingdom". In other words, air carriers that store PNR data outside the EU (as is the case since air carriers may have outsourced data storing capabilities to global distribution systems) will share the data regardless of where it is stored.

[94] Opinion 1/15 cit. para. 200. See also *Ligue des droits humains* cit. para. 218.

[95] *Ligue des droits humains* cit. para. 219.

[96] *Ibid*. The requirement of an independent administrative body as part of the ex-ante review of access requests is discussed in Section III.

that the PNR data of one or more passengers might make an effective contribution to the attainment of the purposes set out in Article 544".[97] Leaving aside the question on the compatibility of processing for "border check" purposes with the CJEU's findings, making the subsequent access to data conditional on new circumstances seems to satisfy access requirements laid out by the CJEU. But the detail is missing here. To justify the subsequent access to data for activities related to terrorist offences, the effective contribution of the data to combat those activities must be considered.[98] The CJEU did not seek this condition for all terrorist offences – only those threatening national security, defence, or public security interest.[99] To justify subsequent access to data for serious crimes, the CJEU gave a different reading of those circumstances, presumably due to the lesser risk that those crimes pose to public security than terrorist offences.[100] Access to combat serious crimes, the Court held, must be granted only to the data of individuals suspected of involving in the relevant crime.[101] To satisfy the latter requirement, the CJEU read the terms "sufficient grounds" and "reasonably" found in the EU PNR Directive jointly and noted that they condition access to data for serious crime based on objective evidence capable of giving rise to a reasonable suspicion that the individual involved in the commission of a serious crime.[102] While the TCA requires the existence of objective grounds, it does not reference the observance of reasonable suspicion in granting access to the retained data for a serious crime.

In relation to the ex-ante review, the TCA subjects access to PNR data to a priori review by a court or an independent administrative body upon request by the Home Office submitted based on "[UK] legal framework of procedures for the prevention, detection, or prosecution of crime".[103] This review requirement is in addition to the power of the Home Office as the PIU to grant access to complete PNR data after the first six months of the five-year retention period.[104] While the text of the TCA seems to incorporate the review requirements noted by the CJEU, the extent to which this review observes the independence requirement is yet to be seen. As mentioned in Section III, there are issues over

[97] Art. 533(1) of EU-UK TCA cit.

[98] *Ligue des droits humains* cit. para. 221.

[99] *Ibid*.

[100] Cf. Case C-203/15 *Tele2 Sverige AB v Post–och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* ECLI:EU:C:2016:970 para. 119; Case C-746/18 *Prokuratuur (Conditions of Access to Data relating to Electronic Communications)* ECLI:EU:C:2021:151 para. 50.

[101] *Ligue des droits humains* cit. para. 221.

[102] *Ibid*.

[103] Art. 533(2) reads that "[u]se of PNR data by the United Kingdom competent authority in accordance with paragraph 1 shall be subject to prior review by a court or by an independent administrative body in the United Kingdom based on a reasoned request by the United Kingdom competent authority submitted within the domestic legal framework of procedures for the prevention, detection or prosecution of crime, except [...] (b) for the purpose of verifying the reliability and currency of the pre-established models and criteria on which the automated processing of PNR data is based, or of defining new models and criteria for such processing".

[104] Art. 552(3) of EU-UK TCA cit.

the oversight of PNR data sharing, and the CJEU case law proves that the adequacy question is not detached from the discussions over oversight mechanisms.

Overall, there is evidence in the TCA of the shifting of PNR data that might ultimately undermine the level of protection afforded to individuals. The next section questions the unchallenged notion that PNR data are processed for *criminal justice* purposes.

V. PNR data processed for criminal justice *or* border control?

V.1. Overview of EU law

As indicated in Section II, PNR is made up of numerous elements of personal data provided by passengers when seeking to book travel but unverified by either the private sector to which they are provided by the data subject or the public sector, which requires the private sector to transmit them on request. The inherent relationship of PNR with the crossing of international borders[105] is obvious from the perspective of the data subject. People do not generally provide their data to travel companies unless they are planning to travel. The obligation to provide personal data to these companies only arises in the process of concluding a contract to travel between the parties. Further, the obligation is primarily one related to travel across international borders, internal border travel does not necessarily require prospective passengers to provide the travel company with PNR data (though this depends on national law). Thus, from the perspective of the individual providing the data and the travel company collecting and processing it, the objective is related to travel which includes border crossing. For the individual providing it, the data is part of the contract with the company, for the company the collection of the data is generally justified based on improving the travel experience of the customer.

As mentioned in Section IV, the CJEU made a very pertinent finding in *Ligue des droits humains* regarding the application of EU data protection standards to this area of rather opaque private-public collaboration.[106] In short, it held that private companies which are required by the state to transfer PNR data to them, do so subject to the high EU standards of the GDPR.[107] When states receive this data for the purposes of fighting serious crime and terrorism, they may use it subject to the less strict rules of the LED.[108] But once the personal data is in the hands of the State authorities, data protection becomes uncertain.

Thus, when the State authorities require companies to transmit PNR data to them, the purpose becomes less clear. It might seem self-evident that there is a border control element central to the objective of the authorities in obtaining PNR data after all the data

[105] A slightly different situation applies to intra-EU PNR where the data relates to the intra-Member State travel and is not limited to Schengen States where border controls on persons have been formally abolished.

[106] *Ligue des droits humains* cit. para. 84.

[107] *Ibid.* para. 81.

[108] *Ibid.* para. 80.

was created for this purpose. Perhaps the use of the phrase "an objective link, even if only indirect one, with air travel" largely cited in *Ligue des droits humains* as part of the ground for the legality of untargeted use of PNR data for the purposes of combatting serious crime or terrorism, is an inversion of sorts of this relationship between travel and extensive use of personal data without consent.[109] But there is a great reluctance on the part of European authorities to admit this at least formally. Instead, European authorities insist that the purpose is to prevent, detect, investigate, and prosecute terrorist offences or serious crimes.[110] Indeed, the CJEU found that this use is specifically unlawful.[111] In the agreements the EU has entered into with third countries (Australia, Canada and the USA) regarding PNR data exchange, the same insistence on the objective as one of serious criminal law and counter-terrorism is maintained. So it is no surprise to find the PNR provisions of the TCA in Part III of the agreement, law enforcement and judicial cooperation in criminal matters, art. 542 et seq. Art. 544 states that the UK "shall ensure that PNR data received pursuant to this Title is processed strictly for the purposes of preventing, detecting, investigating or prosecuting terrorism or serious crime and for the purposes of overseeing the processing of PNR data within the terms set out [in the TCA]".

The reason for the insistence of EU institutions and the UK on the criminal justice purpose of PNR data collection and exchange is evident from the legal bases of the TCA and other international PNR agreements. Leaving aside the somewhat vexed question of what the legal basis of the TCA is anyway,[112] its criminal justice provisions refer back to EU competence under art. 82 TFEU judicial cooperation in criminal matters rather than art. 77(1)(a) and (b) TFEU which create competence to develop a policy on the crossing of external border controls and integrated management of external border controls. The EU's power to adopt legislation depends also on the integration of the Schengen *acquis*

[109] *Ibid.* para. 191: "[i]n addition, in order to satisfy the requirement as to the targeted, proportionate and specific nature of the pre-determined criteria, the databases referred to in paragraph 188 above must be used in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air".

[110] Art. 6(b) of EU PNR Directive cit.

[111] *Ligue des droits humains* cit. para. 288: "...national legislation authorising the processing of PNR data collected in accordance with that directive, for purposes other than those provided for therein, namely for the purposes of improving border controls and combating illegal immigration, is contrary to Article 6 of the said directive, read in the light of the Charter".

[112] See P van Elsuwege, 'A New Legal Framework for EU-UK Relations: Some Reflections from the Perspective of EU External Relations Law' (2021) European Papers www.europeanpapers.eu 785. According to the Commission, "[t]he Commission is of the view that the Agreement with the UK can be concluded as an EU-only agreement since it covers only areas under Union competence, be it exclusive or shared with the Member States. The Commission has chosen Article 217 TFEU as the legal basis for the conclusion of the Agreement. This requires the unanimous agreement of the Member States in the Council and the consent of the European Parliament". See European Commission, 'Questions & Answers: EU-UK Trade and Cooperation Agreement (QANDA/20/2532)' (24 December 2020) ec.europa.eu. See art. 217 TFEU.

into EU law and whether a border control-related measure is an extension of that *acquis*.[113] The UK, while still a Member State, spent much effort avoiding participating in measures adopted under art. 77 and kept a very substantial distance from the Schengen *acquis* altogether preferring to retain sovereign control over external borders including those with other (as then was) EU States.[114] As the whole area of border controls and their management is obfuscated by political claims about its role as an inherent part of State sovereignty.[115] Hence, criminal justice cooperation has turned out to be a more palatable choice of the legal basis for PNR data exchanges generally.

But is this position legally sustainable? The first question to resolve is the relationship of border control with law enforcement and in particular criminal justice. In EU law, "[b]order control should help to combat illegal immigration and trafficking in human beings and to prevent any threat to the Member States' internal security, public policy, public health and international relations".[116] Illegal immigration and trafficking in human beings are both framed as criminal law and indeed as far as trafficking is engaged, a directive requires the Member States to create criminal offences in relation to trafficking.[117] The value of the criminal offence of trafficking in human beings for the purposes of using PNR data for serious crime purposes in a cross border context (i.e. with an inherent border control element) is acknowledged by the CJEU when it found that within the limited grounds for which PNR data can be used, that of serious crime, trafficking in human beings is legitimate as such a serious crime.[118] The risk of misuse of personal data obtained from PNR ostensibly accessed on the grounds of serious

[113] The legal basis of the Schengen Borders Code (Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders).

[114] This position was only modified when the UK sought access to the EU Border Agency, Frontex which was rejected by the CJEU on the basis of the UK's rejection of participation in the field of border controls more generally. See Case C-77/05 *UK v Council* ECLI:EU:C:2007:803.

[115] A particularly good example of this is the Statement of the US Mission to the UN of 7 December 2018 on the Global Compact on Migration. See United States Mission to the United Nations, 'National Statement of the United States of America on the Adoption of the Global Compact for Safe, Orderly, and Regular Migration' (7 December 2018) usun.usmission.gov.

[116] Recital 6 of Schengen Borders Code cit.

[117] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

[118] *Ligue des droits humains* cit. para. 149: "[i]n that regard, as noted by the Advocate General in point 121 of his Opinion, many of the offences listed in Annex II to the PNR Directive – such as human trafficking, the sexual exploitation of children and child pornography, illicit trafficking in weapons munitions and explosives, money laundering, cybercrime, illicit trade in human organs and tissue, illicit trafficking in narcotic drugs and psychotropic substances, illicit trafficking in nuclear or radioactive materials, unlawful seizure of aircraft/ships, serious crimes within the jurisdiction of the International Criminal Court, murder, rape, kidnapping, illegal restraint and hostage-taking – are inherently and indisputably extremely serious".

crime, that is to say the fight against trafficking in human beings, but actually used for border control, is thus very substantial.[119]

The final section examines the place of border control and criminal justice in EU PNR agreements more specifically.

V.2. The juxtaposition of border control and criminal justice in EU PNR agreements

The same intersection of border control, PNR personal data and serious crime is revealed in the other EU agreements on PNR. In the EU-Australia agreement,[120] the objective is strictly limited to preventing, investigating and prosecuting terrorist offences or serious transnational crime.[121] Yet, the Australian Border Force states: "[a]ccess to Passenger Name Record data by the Department [of Home Affairs] forms an integral component of Australia's intelligence led, risk based approach to border protection"[122] *and* that PNR data facilitates "*undertaking the risk assessment and clearance of all passengers arriving into and departing from Australia*".[123] Thus while the stated objective of the agreement is strictly limited to criminal justice, the agency with access to PNR data states its importance for border and immigration control purposes. In the EU-Canada agreement (expired) the objective is serious crime (see above regarding this agreement). Finally, in the third agreement, EU-US,[124] the objective is to prevent, detect, investigate and prosecute terrorist offences and related crimes but then includes a clear border control element that PNR data may be used "by DHS [Department of Homeland Security] to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination".[125]

For the purpose of EU law, the CJEU has held that the legal basis for a measure (including an agreement such as the TCA) is to be assessed in accordance with objective factors such as the purpose of the measure and its content.[126] Its use is also important – what is the actual use of the agreement. From this perspective, efforts to detach PNR Agreements from border control may not be tenable. If PNR is indeed primarily a border control tool because of its relationship with travel and the crossing of international borders as well as how it is used by States for border control purposes, notwithstanding the link between border control and criminal justice, this has important consequences for the legality of PNR data sharing between the EU and the UK. Personal data protection in

[119] See for instance Information Commissioner's Office, *Mobile Phone Extraction by Police Forces in England and Wales Investigation Report*, ico.org.uk.

[120] EU-Australia PNR Agreement cit.

[121] Art. 3 of EU-Australia PNR Agreement cit.

[122] Australian Border Force, *Collection of Passenger Name Records*, www.abf.gov.au.

[123] *Ibid*. (emphasis added).

[124] EU-US PNR Agreement cit.

[125] Art. 4(3) of EU-US PNR Agreement cit.

[126] Case C-479/21 *SN & SD* ECLI:EU:C:2021:929.

border control contexts in UK law is most noticeable by its absence. The Data Protection Act 2018 specifically exempts all border and immigration control processing of personal data from protection under the act (see below). Thus, all the GDPR rules on personal data do not apply to data collected in this context. While specialist agencies did bring this issue to the attention of Parliament at the time of the passing of the legislation, no correction succeeded. Brexit, however, resulted in this failure to receive judicial consideration. The UK NGOs, the Open Rights Group and the 3 Million, which engaged in protecting the rights of EU nationals in the UK post-Brexit, challenged the exemption.

Accordingly, in 2021 the UK Court of Appeal struck down the immigration exemption in the (UK) Data Protection Act 2018, which allows the UK immigration authorities to bypass and restrict fundamental data rights where compliance would be prejudicial to the maintenance of effective immigration control.[127] The Court suspended the effect of its judgment allowing the Home Office until 31 January 2022 to remedy the unlawfulness through legislation. As a result of the UK court judgment, when the EU issued its adequacy decision on data sharing between the EU and the UK necessary for the exchange of personal data between the two, it carved out immigration-related data from its otherwise favourable decision.[128] The consequence of the carve-out is that immigration-related data sharing can take place only based on arts 45-49 GDPR, relating to data sharing with third countries. If PNR is indeed border control (i.e., immigration-related) data sharing, then it would be caught by these restrictions.

The UK government then presented a statutory instrument which purports to remedy the shortcomings of the immigration exemption in the DPA.[129] The new SI has been described as inadequate by the organisations which brought the claim to the Court of Appeal in the first place.[130] The main complaint is that the revised regulations do not fulfil the necessary criteria of being clear and precise, nor do they provide foreseeability for individuals affected as the CA required in its judgment. They also do not fulfil the requirements of GDPR according to the complainants.

VI. Conclusion

There have been 20 years of difficult evolutions taking place towards the EU's global approach to PNR. This *Article* considered the PNR provisions of the EU-UK TCA based on the ongoing conflicts on international data transfers and the effect of characterising PNR data

[127] See in particular Court of Appeal (England and Wales), *Open Rights Group & Anor, R (On the Application Of) v The Secretary of State for the Home Department & Anor* (2021) EWCA Civ 800.

[128] Communication COM(2021) 4801 final from the Commission implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 cit.

[129] The Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022 of United Kingdom.

[130] The 3 Million, *Second Judicial Review Hearing to Challenge Immigration Exemption in Data Protection Act*, the3million.org.uk.

sharing as part of the criminal justice cooperation on future data transfer conflicts. It sketched the multiple layers of PNR governance under the TCA, which eventually raises the question about the transparency and accountability of PNR data sharing carried out accordingly. Moreover, the rules on the scope of PNR data covered by the TCA and the purposes for which the data may be processed call the legality of the PNR provisions of the Agreement into question for their compatibility with EU law. The main issue is the extent to which they afford adequate protection to data subjects compared to the protection afforded under EU law. The starting point in assessing the adequacy standard of the TCA's PNR provisions is the EU constitutional framework ensuring the rights to privacy and data protection. This *Article* argued that in three main areas, the PNR provisions' adequacy to protect data subjects is questionable. The first area is the layers of oversight that the TCA establishes specifically on the processing of PNR data (e.g. PIU as the competent authority and independent administrative body for the ex-ante review of PNR processing) and more generally on the implementation of the TCA's law enforcement section where the PNR provisions are located. On its face, the TCA satisfies the EU requirements of oversight for the former as it largely mirrors the CJEU's findings on the topic in Opinion 1/15. Still, the extent to which the relevant oversight bodies can be deemed independent in practice is yet to be seen. The concerns with the independence and effectiveness of oversight bodies are compounded by the cumulative layers of checks and balances and the absence of transparency (as seen in the initial review of the implementation of the PNR provisions and the decision to extend the interim period).

The second area where the PNR provisions adequacy standard is questioned relates to how the TCA sets out the purposes of data processing and the conditions for the subsequent access to data. The CJEU's findings on these issues in Opinion 1/15 and subsequently in *Ligue des droits humains* suggest that the TCA falls short of satisfying the EU fundamental rights requirements for its failure to condition access to the data for countering serious crimes that have an objective link with the air travel. It also does not require subsequent access to the data based on a reasonable suspicion that the individual in question must involve in the commission of a serious crime. Finally, the legal basis for PNR provisions appears to be vulnerable if PNR data is border control. Its characterisation in criminal justice is through the capacity of the data to be incorporated in border control proceedings to consider the general grounds for refusal of entry into the country.

To ensure the continuity of PNR data transfer in accordance with the EU legal framework, the PNR provisions of the TCA or any future cooperation on the subject must be aligned with the EU fundamental rights framework as interpreted by the CJEU. In this regard, oversight emerges as a major accountability issue. Any future collaboration must disentangle the multiple layers of oversight and ensure they meet the independence requirement put forward by the CJEU and the ECtHR. Serious crime related data processing purposes must be reconsidered in light of the limitations set out in the CJEU's case law. These issues indicate that the PNR provisions of the TCA might not be the end of how EU-

UK PNR data sharing will be governed post-Brexit, and instead, they are the sight of impending discussions. For the continuity of the EU-UK data sharing, including PNR data, the UK must ensure that the UK law is consistent with the EU's adequacy standards, including the CJEU evolving case law. The Data Protection and Digital Information Bill and a sea of uncertainty regarding the "bonfire of retained EU law" indicate that Parliament is willing to take the opposite route to the detriment of maintaining the UK's adequacy standards. This direction might ultimately create uncertainty on the continuity of the free data flow for the public and private sectors.