



Japan-EU Passenger Name Record Negotiations and Their Implications

Toru Maruhashi

► To cite this version:

Toru Maruhashi. Japan-EU Passenger Name Record Negotiations and Their Implications. 14th IFIP International Conference on Human Choice and Computers (HCC), Sep 2020, Tokyo, Japan. pp.100-114, 10.1007/978-3-030-62803-1_9 . hal-03525252

HAL Id: hal-03525252

<https://inria.hal.science/hal-03525252>

Submitted on 13 Jan 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Japan-EU Passenger Name Record Negotiations and their Implications

Toru Maruhashi [†] [0000-0001-8982-6578]

[†] Meiji University, Kanda-Surugadai, Chiyoda-ku, Tokyo 101-8301, Japan
torumaruhashi@meiji.ac.jp

Abstract. EU and Japan started negotiations of an agreement on passenger name record (“PNR”) while EU-CANADA PNR negotiations are concluding. Responding to the call from United Nations Security Council, International Civil Aviation Organization is discussing amendments on the PNR to the Standards and Recommended Practices on Facilitation. In these bi-lateral and global circumstances, what should be desirable outcome of negotiations on Japan-EU PNR Agreement and could be broader issues left behind?

In this contribution, PNR and the nature of its processing are overviewed (Section 2), and their current legal and practical framework in Japan is critically confirmed (Section 3). Then Japanese PNR system is compared with the original draft negotiating directive of Japan-EU PNR Agreement with author’s perspective (Section 4) and finally global implications for the PNR and importance on (relatively legacy) technology and practice of algorithmic pattern-based search are explored.

Keywords: Passenger Name Record (PNR), PNRGOV, Pattern-based search, Transparency

1 Introduction

On 26 July 2017, the Grand Chamber of Court of Justice of the European Union (“CJEU”) delivered Opinion 1/15¹. The Court declared that the envisaged agreement between European Union and Canada on the transfer and processing of passenger name record data (“PNR data” or “PNR”) is incompatible as to sensitive data possibly included in the PNR. It also instructed that various other points must be amended to be compatible with Articles 7 and 8, and Article 52(1) of the Charter of Fundamental Rights (“CFR”).

In July 2019, EU and CANADA jointly declared that they have concluded negotiations for a new PNR Agreement while Canada noted its requirement for legal review².

Globally, International Civil Aviation Organization (ICAO) has been working on new standards and recommended practices (SARPs) on PNR to be contained in Section

¹ CJEU *Opinion 1/15* ECLI:EU:C:2017:592. See Maruhashi T (2019) Draft PNR Agreement between CANADA and EU; CJEU Opinion 1/15 - Distance from Mass Surveillance and Data Retention –. Information Network Law. 17:63–91.(in Japanese)

² Para. 11 of Canada-EU Summit Joint Declaration July 17-18, 2019, Montreal.

D, Chapter 9, Annex 9 to the Chicago Convention responding to the call by United Nations Security Council Resolution 2396. European Commission has been participating in that SARPs' drafting process following the negotiation position approved by Council.³ The draft SARPs seems to incorporate various points from that EU position.⁴

Japan has been on the EU waiting list for the negotiations on PNR Agreements next to Canada.⁵

The Article 37 of Japan-EU Strategic Partnership Agreement ("Japan-EU SPA") is explicit on the partners' endeavour to use PNR.⁶

European Commission, without waiting its conclusion of PNR Agreement with Canada, recommended the Council to authorise the opening of negotiations for Japan-EU PNR Agreement with negotiating directives ("NDs")⁷.

In these bi-lateral and global circumstances, what should be desirable outcome of negotiations on Japan-EU PNR Agreement and could be broader issues left behind?

PNR is a unique set of personal data in several dimensions. These data are internationally transferred from private operators to governments. They are used and analysed for governmental purpose of preventing and combating terrorism and other serious transnational crime. That analysis involves some extent of algorithmic profiling and prediction. They are further transferred to another domestic or foreign government. If we find problems or shortcomings in these processing, that could generally be applicable to other kind of data similarly situated and the way of their regulation.

In this contribution, PNR and the nature of its processing are overviewed (Section 2), and their current legal and practical framework in Japan are critically confirmed

³ Council Decision (EU) 2019/2107, which preamble 14 states "The position of the Union is established in accordance with the applicable Union legal framework on data protection and PNR data, namely Regulation (EU) 2016/679, Directive (EU) 2016/680 and [PNR] Directive (EU) 2016/681, as well as the Treaties of the European Union and CFR as interpreted in the relevant case law of the CJEU, in particular Opinion 1/15".

⁴ Proposed by a task force in ICAO information paper FALP/11-IP/1(December 2019) and approved with amendments at ICAO Facilitation Panel Eleventh Meeting. See Meeting Report FALP/11 (January 2020).

⁵ A. Iizuka, Director of the Customs and Tariff Bureau, Ministry of Finance (Government response in the Diet on 23 March 2018 in Japanese). European Commission expressed its view on the negotiations that "Having arrangements in place in time for the 2020 Olympics would bring a real security dividend." in its Twentieth Progress Report towards an effective and genuine Security Union COM(2019) 552 final 30.10.2019

⁶ Japan-EU Strategic Partnership Agreement was signed in July 2018 and partly became effective on 1 February 2019. Its Article 37 reads 'The Parties shall endeavour to use, to the extent consistent with their respective laws and regulations, available tools, such as passenger name records, to prevent and combat acts of terrorism and serious crimes, while respecting the right to privacy and the protection of personal data'.

⁷ European Commission, COM(2019) 420 final (September 2019). The Economic and Financial Affairs Council authorised revised version of the NDs (12762/19 + ADD 1) on 18 February 2020, which is still confidential as of 24 June 2020. *See also* EDPS Opinion 6/2019 on the negotiating mandate of an Agreement between the EU and Japan for the transfer and use of Passenger Name Record data 25-Oct-2019, available at https://edps.europa.eu/data-protection/our-work/publications/opinions/eu-japan-passenger-name-record-data-agreement_en.

(Section 3). Then Japanese PNR system is compared mainly with the original draft NDs of Japan-EU PNR Agreement with author's perspective (Section 4) and finally , global implications for the PNR and importance on (relatively legacy) technology and practice of algorithmic pattern-based search are explored.

2 PNR and the nature of its processing

2.1 Passenger Name Record

PNR “is the generic name given to records created by the aircraft operators for each flight a passenger books. PNR records contain information provided by the passenger and information used by the aircraft operator for their operational purposes.”⁸ Contracting States of ICAO requiring PNR access should align their data requirements and their handling of such data to guidelines contained in ICAO Document 9944 (ICAO-WCO-IATA PNR Guidelines).

2.2 PNR push and PNRGOV standard

Governments use PNR to conduct analysis that helps to identify possible high-risk individuals that may have been otherwise unknown to government authorities and make, where appropriate, the necessary interventions. PNR information can be provided by aircraft operators by sending the information electronically (“push” method) or allowing the appropriate authorities to access the parts of their reservation systems where the PNR information is stored (“pull” method). However, internationally there is an agreement to utilize the “push” method, for data privacy reasons.⁹

To ensure interoperability for reporting to the appropriate government authorities, a push method message format called PNRGOV based on EDIFACT rules and syntax is developed ‘as the international standard that must be used for the transmission of PNR’¹⁰. The standards¹¹ contains complete description of the message structure, segments and elements as well as the relationship between messages.

2.3 Targeting

Each passenger's PNR data is transferred using push or pull method from the airline's reservation system to the border authority's system such as immigration and customs

⁸ Management Summary on Passenger-related Information [‘Umbrella Document’ version 2.0 – July 2017] published by the International Civil Aviation Organisation (ICAO), the World Customs Organisation (WCO) and the International Air Transport Association (IATA).

⁹ *Ibid.*

¹⁰ *Ibid.*

¹¹ See PNRGOV EDIFACT Message Implementation Guides updated, available at <https://www.iata.org/en/publications/api-pnr-toolkit/#tab-3>.

before entry and departure. In the relevant system, the risk of a passenger is automatically evaluated by a program that incorporates an algorithm or scenario for matching the pattern of high-risk persons, as a pre-processing step called targeting. Once targeted by the risk evaluation process, further risk assessments and investigations are performed and the corresponding passengers are taken additional interrogation at entry and exit. Explanations on Canadian and the US examples of these pattern-based (or rule-based) searches¹² follow:

*The Scenario Based Targeting (SBT) program of Canada Border Services Agency uses advanced analytics to evaluate [PNR] against a set of conditions or scenarios, [which are] made up of personal characteristics derived from [PNR], such as age, gender, travel document origin, places visited and length and pattern of travel. If an individual matches a scenario, further manual risk assessments are conducted by National Targeting Centre officers. Risk assessments include checking individuals against international and domestic law enforcement and intelligence partners' databases, and may result in the individual being referred as a "target" for closer questioning or examination by a Border Services Officer at the port of entry.*¹³

*The Department of Homeland Security (DHS) U.S. Customs and Border Protection (CBP) operates the Automated Targeting System (ATS) [to manage] the shared threat to the homeland posed by individuals ... that may require additional scrutiny prior to entering or exiting the United States. [In identifying such individuals] ATS compares existing information about individuals [including PNR] ... entering and exiting the country with patterns identified as requiring additional scrutiny. The patterns are based on CBP Officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence*¹⁴.

In the latter example of the U.S. ATS, currently PNR is just one of the various source information ingested to the system; other information comes from, for example, Border Crossing Information (BCI), Electronic System for Travel Authorization (ESTA), Secure Flight Passenger Data (SFPD).

¹² See Zarsky TZ (2013) Transparent predictions. U Ill L Rev 1503, arguing importance of modest transparency in prediction process focusing on pattern-based searches.

¹³ Office of the Privacy Commissioner Canada, 2016-17 Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act and the Privacy Act.

¹⁴ Privacy Impact Assessment Update for the Automated Targeting System DHS/CBP/PIA-006(e) January 13, 2017

3 Current legal and practical status of PNR in Japan

In Japan PNR is collected through NACCS system¹⁵ operated by Nippon Automated Cargo And Port Consolidated Systems, Inc.¹⁶ Airline operators are obligated to report PNR in a format designated for NACCS directly or indirectly through its Service Provider¹⁷ in EDIFACT based PNRGOV format to NACCS. Relevant user authorities such as Immigration Service Agency (“ISA”), and Customs and Tariff Bureau, Ministry of Finance (“Customs”) pull PNR reported to NACCS center as described in more detail below.

3.1 PNR and Immigration Control

According to Paragraph 8 of Article 57 of the Immigration Control and Refugee Recognition Act (“ICRRA”)¹⁸, an Immigration Inspector may request to report inbound PNR if he or she finds it necessary for securing the enforcement of landing examination ... from an aircraft operator, a chartered aircraft operator or a joint carrier.

PNR under ICRRA are matters relating to (i) the person making the reservation, (ii) the details of the reservation pertaining to (i), (iii) the baggage of (i) and (iv) the procedures for (i) to board the aircraft. PNR entries are detailed in its Regulation¹⁹.

Inbound PNR shall be reported within 60 minutes from the request. From 1 January 2016, inbound PNR became able to be reported to immigration authorities through NACCS; since then they have had electronic access to PNR reported to NACCS.

3.2 PNR and Customs

The Customs Law (“CL”)²⁰ covers both inbound and outbound PNR.

According to Paragraph 12 of Article 15 of CL, a Director-General of Customs-house (“DG Customs”) may request to report inbound PNR if he or she finds it necessary for securing the enforcement of Article 69-11 (embargoed goods on import) or other provisions of CL, from an aircraft operator or a joint carrier and according to Article 15-3, from a chartered aircraft operator.

¹⁵ NACCS is a system for online processing of procedures taken with Customs, ISA and other relevant administrative authorities or related private-sector services for arriving/departing ships and aircraft or import/export cargo. See The service homepage, available at <https://bbs.naccscenter.com/naccs/dfw/web/> (Japanese)

¹⁶ A Special Corporation governed by Act on Processing, etc. of Business Related to Import and Export by Means of Electronic Data Processing System (Act No. 54 of 1977)

¹⁷ Currently only ARINC can connect NACCS Center for PNR “Push”.

¹⁸ Cabinet Order No. 319 of October 4, 1951

¹⁹ Regulation for Enforcement of the Immigration Control and Refugee Recognition Act (Ministry of Justice Order No. 54 of 1981)

²⁰ Act No. 61 of 1954

According to Paragraph 3 of Article 17 of CL, DG Customs may request to report outbound PNR for securing the enforcement of Article 69-2 (embargoed goods on export) or other provisions of CL, from an aircraft operator or a joint carrier and according to Paragraph 2 of Article 17-2, from a chartered aircraft operator.

Under CL, both inbound and outbound PNR are (i) names of the personal who reserved the tickets, (ii) the details of the reservation, (iii) their accompanying luggage, and (iv) any information with regard to boarding procedures. PNR entries are detailed in Cabinet Order²¹ and Ordinance²².

The Passenger and the Reservation Information shall be reported within 60 minutes and the Belongings and Check-in Information shall be reported within 30 minutes from the request.

Inbound PNR has been available for DG Customs' request since October 2011 and electronically through NACCS since April 2015. Outbound PNR has been available for DG Customs' request since June 2017 and through NACCS since March 2019. In practice, airline operators are required to report both inbound and outbound PNR twice, 72 hours before scheduled time of departure and immediately after the departure.

The major purpose of obtaining outbound PNR is explained as 'grapping the behavior of re-entry passengers by comparing departure information and entry information'²³.

Since March 2019, the electronic reporting of both inbound and outbound PNR through NACCS has been mandatory²⁴.

3.3 Processing of PNR through NACCS

Once an airline operator inputs PNR directly or indirectly to NACCS, it satisfies legal "push" requirement under ICRRRA and CA.

NACCS just operates as a common proxy server making PNR received from airline operators available for ISA and Customs to "pull" it for these authorities' statutory purpose. PNR is just retained in NACCS for six days according to the business process specification specified by the Customs²⁵.

Headings for PNR in NACCS format mainly consists of brief texts, numbers and IATA codes, but exceptionally, two headings of 'other information' are in free text format and can be long one, corresponding to SSR and IFT tags in Segment Group 1 of PNRGOV.

²¹ Cabinet Order No.150 of 1954

²² Regulation for Enforcement of the Customs Law (Ministry of Finance Order No. 55 of 1966) ("RECL")

²³ 'Enhancement for Reporting Scheme of "Advance Information on Passenger" (ANNEX)' presented by Customs to Customs Subcommittee, Tariffs and Foreign Exchange Committee 24 Nov 2016 (in Japanese)

²⁴ Section 14, Article 15 of CL and Article 2-5 of RECL. *See also* Enhancement of Reporting Scheme of Advance Electronic Information (AEI) on Passengers and Crews (May 2017), available at <https://www.customs.go.jp/mizugiwa/ryogu/kekka03.pdf>

²⁵ https://bbs.naccscenter.com/naccs/dfw/web/data/customs/jimu/toriatsukai_index_tetsu_k_1.html (in Japanese)

NACCS allows airline operators to push their PNR in PNRGOV format processed based on PNRGOV standard.

Japanese PNR system is compatible with ICAO-WCO-IATA PNR Guidelines.

3.4 Retained PNR as Personal Information File

Particulars of PNR collected by ISA and Customs shall in accordance with Articles 10 and 11 of the Act on the Protection of Personal Information Held by Administrative Organs (APPIHAO) be notified to Ministry of Internal Affairs and Communications (MIC) and published as a Personal Information File (PIF) Register, elements of which includes:

Name of the PIF; Name of the Administrative Organ and the name of the organizational section in charge of the processes for which the PIF will be used; Purpose of Use of the PIF; Particulars recorded in the PIF; the scope of individuals that are recorded in the PIF; The means of collecting the Personal Information recorded in the PIF; Whether the Recorded Information contains Special Care-required Personal Information; If the Recorded Information will be routinely provided to a party outside the Administrative Organ, the name of that party.

However, PIF is exempted from these notice and publication requirement (Articles 10(2) and 11(2) of APPIHAO), if it contains particulars concerning the security, diplomatic secrets, and other important interests of the State or it is prepared or obtained for criminal investigation, investigation of tax crimes based on the provisions of laws related to tax, or instituting or maintaining a legal proceeding.

Processing and retention of PNR are governed by APPIHAO and Public Records and Archives Management Act (“PRAMA”). Individuals (including foreign nationals living abroad) have in principle a right to disclosure, correction (including deletion) and suspension of use or provision under the APPIHAO²⁶.

Under Article 5 of PRAMA, when an employee of an administrative organ has prepared or obtained an administrative document, the head of administrative organ must set the retention period of document and the date on which the relevant retention period expires.

Current retention period of PNR seems to be 5 years (ISA) and 7 years (Customs) respectively according to Administrative Document File Management Registry. After the retention period, they will be deleted outright. Unlike EU-Canada PNR agreement, no masking operation is used.

²⁶ See preamble 165-170 of Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (“Adequacy Decision”)

3.5 PNR transparency/data minimisation

According to Article 49 of APPIHAO, the MIC "may collect reports on the status of enforcement of this Act from the heads of Administrative Organs" and annually publishes a summary of the reports.

The PIFs on PNR of ISA and Customs describes their purposes as 'equitable control over the entry into and departure from Japan and residence of all persons' and 'prevention of embargoed goods from importation into Japan etc.' respectively; both of them do not contain Special Care-required Personal Information i.e. sensitive information nor routinely provided to other administrative organs.

Data formats of Japanese PNR is compatible with ICAO-WCO-IATA PNR Guidelines and can be processed based on PNRGOV standard through NACCS. To achieve data minimisation, some 'other information', which are expected as filled in free text information corresponding to SSR and IFT tags in Segment Group 1 of PNRGOV shall be automatically filtered out through NACCS processing.

Customs publish a webpage entitled 'Summary of Passenger Name Record (PNR)'²⁷ and specifies the purpose of use of transmitted PNR as "customs enforcement purpose including preventing the smuggling of terrorism related goods and illicit drugs".

3.6 Targeting use

PNR has been analyzed for purposes of immigration and customs examination, but there is little public information about how it has been used and useful for targeting purposes, other than just for blacklist matching by supplementing it with other information such as Advanced Passenger Information.

According to Basic Plan for Immigration Control and Residency Management²⁸, as to the use of PNR, its "Immigration Control Intelligence Center²⁹ ... receive PNRs [through NACCS since January 2016] and, then become able to conduct advanced analysis using the information held by the Ministry of Justice along with other information, and these results are being used in the border measures by the regional immigration control and residency management offices at the port of entry".

ISA "conduct[s] advanced analysis using [PNR] held by [it] along with other information, and these results are being used in the border measures by the regional immigration control and residency management offices at the port of entry... [, and is] taking measures to identify persons who pose a security risk, ...and preventing their entry, and will continue to strengthen use of such information and to conduct smooth and prompt entry examinations for foreign nationals who do not pose a problem."³⁰

²⁷ https://www.customs.go.jp/english/procedures/advance4_e/index_e.htm

²⁸ http://www.immi-moj.go.jp/seisaku/pdf/2019_kihonkeikaku_english.pdf

²⁹ A Passenger Information Unit (PIU) for ISA.

³⁰ Ministry of Justice 'Basic Plan for Immigration Control and Residency Management (April 2019). http://www.immi-moj.go.jp/seisaku/pdf/2019_kihonkeikaku_english.pdf

In September 2019, ISA was “considering the introduction of a system, a so-called rules-based engine that generates automatic trend analysis and categorization of foreigners to be cared and performs automatic matching”³¹. This presumably mean that automated targeting using PNR has not actually progressed at least on the ISA side.

3.7 Sharing and further use by domestic authorities

As to sharing of PNR data with other relevant domestic agencies, “[i]n accordance with the [APPIHAO], [Customs] share PNR data with other relevant government agencies solely to the extent necessary for the customs enforcement purpose including preventing from smuggling of terrorism related goods and illicit drugs and [Customs] determine the necessity of sharing for each case individually”³².

Under ICRRA, the Director-General and other official of ISA are encouraged to share information with relevant governmental agencies (Article 61-7-7), and may request necessary corporation from them (Article 61-8).

APPIHAO does not prohibit an administrative organ from sharing Retained Personal Information (“RPI”) contained in PIF solely for the original purposes, or as otherwise provided by laws and regulations (Article 8(1)).

In addition, an administrative organ may provide another person with RPI for purposes other than the original purpose, if RPI is provided to another administrative organ or local public entity, who uses it only to the extent necessary for executing the processes or business under its jurisdiction provided by laws and regulations, and there are reasonable grounds for the use of that RPI (Article 8(2)(iii)).

Accordingly, Customs or ISA may, within their mandate, share PNR with national or prefectural law enforcement agencies or agencies responsible for national security, and within the latter’s mandate, if there are reasonable grounds for the use of PNR.

However, there are few public records regarding governmental use of PNR for the purpose of law enforcement or national security except for a few examples of an abstract narrative description. In 2019, enormous numbers of foreign dignitaries came to Japan for the emperor’s throne. The National Police Agency reported, “The police collected and analyzed comprehensive terrorism-related information in close cooperation with foreign security intelligence agencies, etc. to prevent illegal acts such as terrorism against these key persons. At the same time, in cooperation with the [ISA] and [Customs]...countermeasures against terrorism, such as border measures, utilizing [PNR] were taken.”³³

Actually, no such out of the purpose sharing is published in the past Article 49 APPIHAO annual summary reports compiled by the MIC.

Probably, police and intelligence agencies actually and routinely have been provided from ISA and Customs and have used PNR for the original purpose, but they do not

³¹ Minutes of the 16th meeting of ‘The seventh Immigration Policy Discussion Panel’ and its material no. 3 ‘immigration control’(19 September 2019) (in Japanese)

³² fn. 27.

³³ "Review and Outlook of Security (2019)", Security Bureau, National Police Agency (in Japanese).

retain PNR as subset of NACCS based database, rather it has somehow been entered as a new entry into or flagged as PNR-originated on an existing entry in their own black lists, or if it is suspect's one, is incorporated into a criminal case records, which is outside the scope of APPIHAO PIF disclosure and reporting scheme.

3.8 Sharing and further use by foreign authorities

Customs share PNR data with other foreign customs administrations, “in accordance with the Article 108-2 of the [CL] and Customs Mutual Assistance (“CMA”) Framework, solely to the extent necessary for the customs enforcement purpose including preventing from smuggling of terrorism and related goods and illicit drugs and [Customs] determine the necessity of sharing for each case individually”³⁴. The nuances of the actual provisions of that Article 108-2 are slightly different; reciprocity principle and its purpose limitations are stated as:

Customs, when sharing information must confirm the foreign counterpart authority can provide the information equivalent to the information to be shared, the same level of confidentiality as in Japan is guaranteed by the laws of the relevant foreign country for the information to be shared, and the information to be shared is not used for any purpose other than contributing to the performance of the foreign counterpart's duties.

Minister of Justice, i.e. ISA can share PNR with other foreign immigration administrations, in accordance with the Article 61-9 of the ICRRA solely for their enforcement purpose and appropriate measures shall be taken to ensure that shared information is not used for purposes other than helping the foreign counterpart authorities execute their duties. Unlike CL, no reciprocity or confidentiality is required here.

As to the privacy and data protection in international agreements, most of the CMA Agreements and Cooperative Frameworks has very simple provisions. For example, Paragraph 2 of Article 16 Japan-European Community on Co-Operation and Mutual Administrative Assistance in Customs Matters provides reciprocally for:

Personal data may be exchanged only where the Contracting Party which may receive it undertakes to protect such data in at least an equivalent way to the one applicable to that particular case in the Contracting Party that may supply it. The Contracting Party that may supply the information shall not stipulate any requirements that are more onerous than those applicable to it in its own jurisdiction. The Contracting Parties shall communicate to each other information on the laws and regulations of each Contracting Party, including where appropriate, those in the Member States of the Community.

Thus, PNR obtained from airline operators may be provided (or feed-backed) from Japan Customs to EU member states customs solely for the latter authority's duty, which is not restricted to prevention of smuggling of terrorism and related goods and illicit drugs.

³⁴ fn. 27.

3.9 Data security; security breach notification.

The head of an administrative organ must take necessary measures to prevent the leakage, loss, damage, and other appropriate management of the RPI (Article 6 of APPIHAO). MIC “Guidelines on Measures for Appropriate Management of Personal Information Held by Administrative Organs” breaks down data security measures and a data breach incident shall be promptly reported to Chief Privacy Officer of the Organ. If the fact on the data breach will be publicly disclosed, the information will be promptly provided to the MIC. If the data breach is caused by staff of the agencies, disciplinary action will be taken (Article 82 of the National Public Service Act) and penalized in case of intentional leakage of confidential information (Article 109 (xii) of the National Public Service Act).

As to access control, Customs disclose, “Limited officials in the centralized unit solely utilize PNR data for analyzing and targeting of passengers. To limit the access to PNR data, the data is used in the closed system and the access to the facility in which the unit is situated and the office of the unit is strictly limited”³⁵. The centralized unit is Passenger Information Unit (“PIU”), though it is not in a cross-agency style.

4 Comparative analyses of EU NDs and Japanese PNR processing legislation and practice

As to PNR negotiations with EU, Japanese government recognises the necessity and importance of the use of PNR (**para. 2 of NDs**).

As a relatively early adapter, Japan has already extended its PNR system coverage to most of the airline operators other than EU-based one. Through NACCS, airline operators are using PNR ‘push’ and can transmit it in PNRGOV standard format twice (72 hours before the scheduled departure time and immediately after the departure) without heavy burden or inconvenience (**paras 10-12**). As far as Japanese laws and regulations are concerned, EU airline operators have a legal basis for them to transfer PNR via NACCS to ISA and Customs (**para. 7**).

The other negotiation points are, as elaborated in Section 3 above and for the reason not controllable by Japanese government, not simple or easy. Author’s perspective follows.

4.1 Purpose limitation (paras. 3 and 5)

Limiting use of PNR for - although Article 37 of Japan-EU SPA is in line with - sole purpose of preventing and combating terrorism and other serious transnational crime defined in EU Legislation, would lessen the discretion of ISA and Customs in using and sharing PNR because they are not subject to any such limitation under Japanese

³⁵ *Ibid.*

laws and regulation. We need special provisions for this limitation under ICRRA and CL.

As to defining the categories of crime, recent working arrangement between NPA and Europol (“WA”) ³⁶ covers exchange of specialist knowledge and strategic analysis on terrorism and serious crime, and lists areas of crime specified by Europol though NPA reserves its position. The list could be a starting point for the negotiations.

4.2 Transfer of analytical information (para. 4)

NDs requires flow of ‘analytical information’ from competent authorities of Japan to police and judicial authorities of the Member States, Europol and Eurojust³⁷. This flow is not specifically covered by any of the previous agreements or frameworks regarding the immigration control or customs. In contrast, WA encourages exchanging analyses, but does not provide for the legal basis for the transfer of personal data. If ‘analytical information’ includes personal information, we need to comply with APPIHAO³⁸.

4.3 Clear and precise safeguards and controls (para 8)

Respect for fundamental rights and freedoms (paras. 3 and 6) As CJEU in its Opinion 1/15 on the envisaged EU-Canada PNR Agreement used the strict necessity test to ensure proportionality of that Agreement to protect fundamental rights and freedoms, we need to and probably it is enough to consider that its guidance is broken down in para. 8.

The categories of PNR, data minimisation and proportionality/Sensitive data. As elaborated in Subsection 3.3 above, Japanese PNR is considered to be already minimised in line with PNRGOV and to be proportionate to the purpose of the PNR Agreement except for headings allowing input of long free text information.

APPIHAO does not prohibit Administrative Organs from processing sensitive data within the meaning of EU law. However, as far as both PIFs are concerned, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning a person’s health or sexual life or orientation cannot on its face be included in headings other than two ‘other information’ headings in free text format.

If the free text information in these headings can be automatically filtered out through NACCS processing, there will be no room for sensitive data remaining in PNR and data minimisation requirement will be satisfied at the same time.

³⁶ Working arrangement on establishing cooperative relations between the National Police Agency of Japan and the European Union Agency for Law Enforcement Cooperation signed on 03 December 2018.

³⁷ From EU to Japan, *See* EDPS Opinion fn. 7 paras 22-23

³⁸ *See* II. (b) (2) Limitations flowing from APPIHAO of Appendix 2 to Adequacy Decision

Data security, security breach notification. The general data security requirement under APPIHAO is as described in subsection 3.9.

Here, the addressees of the data breach notification are designated as European national data protection supervisory authorities; it seems difficult for Japanese PIUs in Customs or ISA to give the notification directly to such supervisory authorities.

A concession would be to construct communication route via Japanese supervisory data protection authorities, if any, or Personal Information Protection Commission (PPC)³⁹ on their behalf.

Transparency, right of Access. As discussed above, transparency to passengers are to some extent achieved by publishing PIFs. In addition, Customs have certain level of notice to the passengers on its website. We shall improve the notification content.

APPIHAO has provisions on right to access, rectification and deletion, where appropriate, however, the problem is how to secure the right of individual notification of the use of PNR as instructed by CJEU⁴⁰ citing analogically *Tele2 Sverige*⁴¹. EU does not legislate in PNR Directive or Law Enforcement Directive⁴² nor included in PNR agreements with the U.S. or Australia this right by which an individual must be notified of the use of information by competent authorities as soon as that information is no longer liable to jeopardise the government investigations. At maximum concession, a mechanism similar to that presented in the Adequacy Decision⁴³ under which an individual who suspects that his/her PNR has been collected or used by public authorities in Japan can submit a complaint to the PPC⁴⁴.

Effective Redress. As to the effective administrative and judicial redress concerning PNR generally, legal framework explained in preambles 11-170 of Adequacy Decision will apply.

Automated Decision-Making, database compared. As preamble 93 of Adequacy Decision describes, Act on the Protection of Personal Information (APPI), APPIHAO nor relevant sub-statutory rules contain general provisions addressing the issue of decisions affecting the data subject and based solely on the automated processing of personal data. We need some regulations on these criteria, especially when ISA introduces ‘rules-based engine’. Although practically PNR targeting would follow human review, algorithms used for pattern-based search for the purpose of targeting and these patterns

³⁹ See Subsection 4.4 below.

⁴⁰ See Opinion 1/15 fn. 1 paras. 221-225, fn. 1

⁴¹ *Tele2 Sverige and Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, (21 December 2016) para. 121

⁴² Directive (EU) 2016/680

⁴³ fn. 26.

⁴⁴ See Adequacy Decision preambles 141-143.

need some scrutiny in various phases of development from political, legal and technological viewpoint as well as ex-post control such as review of usage and production of statistics on false positives and negatives and their disclosure or publication ⁴⁵.

The use of PNR data by the Japanese competent authority beyond security and border control checks. As discussed, ISA and Customs seems to routinely share PNR with police organisations for their original purpose. APPIHAO does not prohibit these agencies from sharing PNR with police to the extent necessary for law enforcement and there are reasonable grounds for the use of PNR. We need to clarify that enriching blacklists used by police with shared PNR needs certain level of additional supervision.

The period of retention of the PNR data. PNR seems to be retained by 5 years (Customs) or 7 years (ISA) respectively and deleted outright upon expiration of these retention periods and no masking operation is used in the interim.

As CJEU does not allow retention of PNR after departure, justification of the purpose of retaining outbound PNR for behavioral analyses for the future re-entry is necessary⁴⁶.

Note that EU PNR Directive obligated PIU to retain both inbound and outbound PNR for 5 years (Article 12(1)). The negotiations in this regard would be highly dependent on the formal outcome of EU-Canada PNR Agreement.

Transfer to other authority, onward transfer. Both ISA and Customs have statutory power to transfer PNR to domestic authorities or foreign counterparts and both of them are obligated to take certain measures to protect confidentiality or purpose limitation. We need to improve the level of protection in such transfer to the one in the PNR Agreement.

For limiting countries to which PNR is transferred to those countries of adequacy decision or concluding PNR agreement, we need to consider if the U.S., Canada, and Australia is sufficient for Japan to exchange PNR.

4.4 Oversight by an independent public authority (para 9)

As explained above, and more thoroughly described in the Adequacy Decision regarding police or intelligence purpose use, PNR obtained by Customs or ISA is under the supervision of several government agencies whose independence is questionable⁴⁷.

⁴⁵ See Zarsky fn. 12

⁴⁶ See fn. 14. “The ATS 15-year retention period is based on CBP’s historical encounters with suspected terrorists and other criminals, as well as the broader expertise of the law enforcement and intelligence communities. It is well known, for example, that potential terrorists may make multiple visits to the United States in advance of performing an attack. It is over the course of time and multiple visits that a potential risk becomes clear.”

⁴⁷ US supervision over PNR has a similar structure that spans multiple agencies. The shortcoming of that structure is criticized by Article 29 working party in its letter of 11 April 2018.

In this regard, since December 2019 Japanese government has been discussing in gathering and consolidating regulations regarding personal information protection relating to the private sector (i.e. APPI), administrative organs (i.e. APPIHAO), and incorporated administrative agencies and toward having the PPC centrally govern the consolidated systems. However, this consolidation process is expected to take long. In the interim, we need to have some tentative solution for independent oversight on PNR.

4.5 Joint Review of targeting algorithm? (para 13)

Presumably, the regular joint review of the PNR Agreement will be conducted at the same level as the Adequacy Decision in general, but a review of the reliability and topicality of PNR targeting may be new thing. It is necessary to prepare for this kind of review of algorithm and develop a supervision strategy.

5 Conclusion

PNR and pattern-based search is developed on the relatively legacy technology. It seems perhaps that relative importance of PNR in the context of combat of terrorism and international organized crime might have been lowered.

Nevertheless, how to control pattern-based algorithmic search by government continues to be important, because, if we cannot control this level of technology and its use by government, we would face much more difficulties in controlling more sophisticated technology based on machine-learning (or artificial intelligence).

If the PNR analysis still has some effectiveness against terrorism and international organized crime, it is undoubtedly important that global development and collaboration supporting UN Security Council Resolutions and the ICAO SARPs discussion.

There is a need to standardize the way of controlling the PNR pattern-based search that should be implemented in democratic countries as well as to increase the number of countries that use PNR globally.

Should the partners of EU PNR Agreements including Japan create a system in which peers review each other in terms of technology and governance of PNR targeting instead of one-way audit of PNR?

There is a need to deepen academic discussions while making efforts to increase the transparency and interpretability of algorithmic decision-making tools, such as statistics on the practicality efficiency and topicality of the PNR.

This paper prioritizes a detailed introduction to Japan's PNR system and does not conduct a deep legal doctrinal analysis. Author believes that this level of detail will work as lenses through which we view possible improvement in processing small set of, but important categories of personal data like PNR. If the conventional and orthodox approach on retaining, processing and sharing personal data by public agencies adopted by Japan will be refined through these PNR negotiations with the EU, it will bring a 'security dividend' to Japanese government and citizens and globally to participants in a forum such as ICAO.

