

Bibliography

1. Article 29 Data Protection working Party, Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf (12.04.2016)
2. BELLANOVA R, The Discreet Charm of Passenger Data. Big Data Surveillance Coming Home, available at: <https://free-group.eu/2016/01/14/the-discreet-charm-of-passenger-data-big-data-surveillance-coming-home/> (12.04.2016)
3. BROWN I/ KORFF D. Foundation for Information Policy Research, Privacy & Law Enforcement, study for the UK Information Commissioner, February 2004. Available at <http://discovery.ucl.ac.uk/3880/1/3880.pdf> (12.04.2016)
4. CITRON D, Technological Due Process, University of Maryland Legal Studies Research Paper No. 2007-26; Washington University Law Review, Vol. 85, pp. 1249-1313, 2007. Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1012360
5. Communication from the commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries (COM (2010) 492 Final), available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52010DC0492> (12.04.2016)
6. Council of Europe Commissioner for Human Rights, Protecting the Right to Privacy in the Fight Against Terrorism, Issue Paper (2008)3, prepared by Douwe Korff, available at: http://insanhaklarimerkezi.bilgi.edu.tr/media/uploads/2015/07/31/Ozel_Hayat.pdf (12.04.2016)
7. EDPS Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 25 March 2011, Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-12-09_US_PNR_EN.pdf (12.04.2016)
8. EU Fundamental Rights Agency, Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the use of Passenger Name Record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (COM(2011) 32 final) Vienna, 14 June 2011, available at: <http://www.statewatch.org/news/2011/jun/eu-pnr-fra-opinion.pdf> (12.04.2016)
9. KORF D. Passenger Name Records, data mining & data protection: the need for strong safeguards, The Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 15 June 2015, Available at: [https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD\(2015\)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf](https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf) (12.04.2016)

10. O'CONNOR R, Is Cameron proposing to legislate, inadvertently, for a Police State in the UK? Why citizens should urge caution, balance and proportionality, 21 January 2015, available at: <http://groovyfuture.com/is-cameron-proposing-to-legislate-inadvertently-for-a-police-state-in-the-ukwhy-citizens-should-urge-caution-balance-and-proportionality/> (12.04.2016)
11. Spanish delegation Note to the EU Council, 5 March 2015, available at: <http://www.statewatch.org/news/2015/mar/eu-council-pnr-mexico-argentina-6857-15.pdf>
12. United States Government Accountability Office Report to Congressional Requesters, Secure Flight – TSA Could Take Additional Steps to Strengthen Privacy Oversight Mechanisms, September 2014, available at <http://www.gao.gov/assets/670/665673.pdf> (12.04.2016)

1. Introduction

Over the last decade and a half much opinion has been expressed and a lot of development has been carried out on the subject of Transmission of Personal Data by Airlines to the states and to the third countries.¹ As the discussions on the topic has not been ended due to current EU Passenger Name Record (PNR) Directive Proposal² and EU-US PNR agreements I would like to point out some highly controversial aspects of the PNR subject rather than a general overview. However before pointing out the core issues, a brief abstract of the debate must be given in order to explain the discussions thoroughly.

Several governments are persuaded that the mass-surveillance of passenger data is a key tool for fighting against terrorism and transnational serious crimes.³ Since the perception of the role of the police has transformed into its being a proactive and intelligence-led activity⁴, the usage of the datasets has been expanded concurrently. That is why governments do not require traditional passenger information such as Advance Passenger Information (API)⁵ and Secure Flight Passenger Data (SFPD)⁶ which both include relatively limited information about passenger to be shared, but PNR.⁷ As Douwe Korff says in his report :

*“The demands for PNR data are part of the wider demands for suspicionless mass collection, retention, and analyses of Data: of e-communications data, financial transaction data and now travellers’ data and, especially, the linking and combining of those data.”*⁸

¹ KORFF, Passenger Name Records, p.4.

² COM (2011) 32 Final.

³ BELLANOVA, The Discreet Charm of Passenger Data, p.1

⁴ BROWN and KORFF, Information Policy Research, p.

⁵ For more information see: https://en.wikipedia.org/wiki/Advance_Passenger_Information_System

⁶ For more information see:

http://www.amadeus.com/corp/xml/documents/aco/gb/en/secure_flight_passenger_data_overview_for_amadeus_customers.pdf

⁷ “In the airline and travel industries, a passenger name record (PNR) is a record in the database of a computer reservation system (CRS) that contains the itinerary for a passenger, or a group of passengers travelling together.” See: https://en.wikipedia.org/wiki/Passenger_name_record

⁸ KORFF, Passenger Name Records, p. 8.

Hence, when we talk about sharing of the PNR data we would be talking about a relatively new dimension of the balance between security and freedom and the Big Data. The discussions on the topic are therefore focused on the legitimacy of the aims, the scope and the usage of the data collected, the safeguards provided and obviously proportionality.

After this short introduction I would like to focus on some main issues more closely. These are:

- i. The risks inherent in the PNR sharing and analysing system,
- ii. The tendency of extension of the list of collection aims,
- iii. The current developments in Turkey

2. Core Issues

2.1. The risks inherent

2.1.1. Mislisting and misidentifying

It is said that two types of error can occur in the screening program⁹. Firstly traveller may be erroneously believed to be a person who actually they are not and secondly they maybe the listed person but they are wrongly assessed and wrongly included in a category.¹⁰ As the profiling system works in a way that *“People who did X and Y often also did Z. You did X and Y, so we will treat you as if you are likely to you are likely to do Z”* the profiling system can make errors a fortiori in a world of massive “Big data”.¹¹

According to a report prepared by US government Accountability Office such systems can help protect against potential act of terrorism that might target the nation’s civil aviation system but, at the same time this can also have potentially inappropriate impact on the traveling public.¹² For example if the algorithm identifies a person as high risk because he/she has a similar name and date of birth with an individual who may be listed on a watch list this may cause delays and some other inconveniences for the person effected¹³. Bearing in mind that a conference organized by Vrije University Amsterdam strikingly named *“Obscured by Algorithm: How to prove yes if computer says no”*¹⁴, one can easily could get a clue about the possible risk of matching PNR data against some other bulk datasets.

To minimize the possible risk of the system it is suggested that profiles should not never be used for trying to “identify” terrorist from a large datasets.¹⁵ One other suggestion is that likelihood of flagging false positives should be reduced by using predefined and fact based

⁹ KORFF, Passenger Name Records, p.18.

¹⁰ KORFF, Passenger Name Records, p.18.

¹¹ KORFF, Passenger Name Records, p.18.

¹² United States Government Accountability Office Report to Congressional Requesters, The report is hereafter referred to as “the GAO Report”.

¹³ GAO Report, p.1.

¹⁴ see: <https://www.youtube.com/watch?v=FV1a5dlTUB8>.

¹⁵ KORFF, Passenger Name Records, p 25.

assessment criteria and by analysing the criteria through testing on anonymised samples.¹⁶ it is also said that some filtering system of the dataset could also help for reducing the possible errors.¹⁷ As Edward Snowden says: *“The problem is that when you collect it all when you monitor everyone you understand nothing”*.

2.1.2. Discrimination

It is pointed out in an article By O’Connor that the practices mentioned above may lead to erroneous conclusions that can result in negative outcomes that affect not only the rights of individuals but also of specific groups.¹⁸ Since the algorithms written by data scientist and programmers, one can not easily make sure that whether or not laws are being followed and rights are sufficiently protected. Some concerns on the accountability also raises as it is recognised that the usage of the technology is could be a way of delegation of legislative power to code writers.¹⁹ Citron goes further and says that programmers inevitably alter established rules when embedding them into code in ways the public, elected officials and the courts cannot review.²⁰ When the algorithms increasingly directs policy decisions, the individuals are less and less able to challenge those results.²¹

When it comes to the PNR data the issue is require more attention as it includes the data such as meal preferences, popular travel destinations or ethnic origin of a person. When this dataset matched against some other dataset which includes let us say the type of websites one has visited or connections to some religious or ethnic groups, the results of the analyse is likely would be a discriminatory labelling.

To minimize the discrimination risk “a new concept of technological due process”²² is proposed. It is also claimed that *“the only way to counter these problems is through full transparency regarding the technologies being used, open peer review by security engineering experts and limits on “Big Data” disclosure and linkages.”*²³ According to FRA it would be useful to create suitable statistics based on PNR data to detect discriminatory patterns in the application of PNR system and this system must be created anonymously to comply with EU data protection principles.²⁴

2.2. The tendency of extension of the aim pursued

¹⁶ FRA Report p.5.

¹⁷ FRA report, p.5.

¹⁸ O’CONNOR, Police State in the UK.

¹⁹ O’CONNOR, Police State in the UK.

²⁰ CITRON, Technological Due Process, from abstract.

²¹ KORFF, Passenger Name Records, p.30

²² “a carefully structured inquisitorial model of quality control [that] can partially replace aspects of adversarial justice that automation renders ineffectual [and that] also provides a framework of mechanisms capable of enhancing the transparency, accountability, and accuracy of rules embedded in automated decision-making systems.” CITRON, Technological Due Process, from abstract.

²³ KORFF, Passenger Name Records, p.36.

²⁴ FRA opinion on PNR, p.10.

As it is increasingly accepted on international level that PNR are necessary tool in the fight against terrorism, more and more countries are now demanding that airlines hand over their passenger information in bulk to them. According to an EU council note Russia, Mexico, United Arab Emirates, South Korea, Brazil, Argentina and Saudi Arabia are among the countries demanding PNR from airlines without even having an agreement like between the EU-US PNR agreement.²⁵

Since the international travel and the amount of passenger rapidly increased, the electronic processing of data before arrival of the passengers largely facilitates security and border control checks. Therefore law enforcement agencies can focus only on those passengers who are believed carry an actual risk to security.²⁶ Besides, most countries including EU members also have an obligation to cooperate with other countries in the fight against terrorism. Due to this reason countries also exchange information that may help in combating against terrorism and serious transnational crime.²⁷ However to comply with the ECtHR principles and other data protection principles in general, the limitation of fundamental rights has to be well justified and its necessity clearly demonstrated so that the system be able to strike a right balance between demands for the protection of public security and the restriction of privacy rights.²⁸

Considering the fact that more limited passenger information such as API and SFPD suffice to meet all the requirements to identify known people who for some reason wanted or looked out for by the authorities, it can be said that the reason behind the demands for PNR is because states want to use this additional data for data mining and profiling purposes so that the probable or potential terrorists can be identified.²⁹ Furthermore, when one think the facts that are exposed by Edward Snowden, it is easily recognizable that the collection of the PNR data is part of the global surveillance programmes that is run across the world in general. Such general surveillance raises serious democratic problems which are not answered by the repeated assertion that “those who have nothing to hide, have nothing to fear.”.³⁰

The main motive for the collection of large datasets for immigration, law enforcement and security purposes came from the terrorist attacks in the USA occurred on 9/11.³¹ However it should be noted that the current developments show that the states use PNR data for aims other than combating terrorism. For example, as Article 29 Working Party has pointed out The EU PNR proposal is not clear about whether the aim is to fight against terrorism and terrorism related crimes only. It is also noted by EDPS that the present proposal does not

²⁵ Spanish Delegation Note to the EU Council, 5 March 2015, p.1

²⁶ COM (2010) 492 Final, p. 5.

²⁷ COM (2010) 492 Final, p.6.

²⁸ Article 29 Data Protection Working Party, Opinion 10/2011 on the proposal for a Directive on the use of passenger name record, p.3 et seq.

²⁹ KORFF, Passenger Name Records, p.8.

³⁰ KORFF, Right to Privacy in the Fight Against Terrorism, p.13.

³¹ KORFF, Right to Privacy in the Fight Against Terrorism, p.3.

affect the possibility of Member States to provide for a system of processing PNR data for purposes other than specified in the proposal.³²

It should be noted that the only legitimate aims for the transferring and sharing of PNR data could be that fighting against terrorism and serious transnational crime³³. Therefore the data should only be transmitted to the relevant law enforcement agency. However it is suffice to not that this is not the case in general.

2.3. The sharing of passenger name record in Turkey and transmission to the Third Countries.

According to the “Ordinance on Responsibilities of Air Carriers” article 9³⁴ like the UK and French, Turkey also requires PNR data to control irregular immigration which is a non-law enforcement activity. But the problem arises from -like before in the era of pre-EU-US PNR agreement- what would happen if there is a conflict of law? EU based airlines should not share PNR data for purposes other than fighting against terrorism and serious transnational crime and to the third countries which does not have an adequate level of data protection. But the air carriers are bound by both Turkish law and the law of respective Member Country. Therefore there must be a harmonization of the systems if the sharing demands have a legitimate aim to be pursued.

Secondly it is also interesting that the mentioned law states that the reason for the collection of PNR data is to control irregular immigration. Therefore, the competent authority is Directorate General of Migration Management (Göç İdaresi Genel Müdürlüğü). It should be pointed out that as well as the aim pursued with the collection is not generally accepted as legitimate, the legal basis of the sharing demand is not an act enacted by parliament. This also would infringe the basic principles of data protection.

³² EDPS Opinion p. 5 et seq.

³³ EDPS Opinion, p.3 et seq.

³⁴ Hava Yolu Taşıyıcılarının Yükümlülüklerine İlişkin Usul ve Esaslar Hakkında Yönetmelik, Turkish Official Gazette, 7 November 2015.