Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Russian PNR system: Data protection issues and global prospects

*Olga Mironenko Enerstvedt**

Norwegian Research Center for Computers and Law (NRCCL), University of Oslo, Norway

Keywords:
PNR
Passenger Name Record
Russia
Privacy
Data protection
Security
Aviation
Personal data

ABSTRACT

The usage of Passenger Name Record (PNR) for security purposes is growing worldwide. At least six countries have PNR systems; over thirty are planning to introduce them. On 1 December 2013, a Russian PNR system will be implemented. But enhanced collection of personal data leads to increased surveillance and privacy concerns. Russian authorities state that passengers' rights will be respected, but a closer look at the Russian regime reveals a number of critical points. From a global perspective, the Russian regime is only one of many PNR systems, including new ones to come in the future. Apparently, for the majority of them, similar challenges and problems will apply. At the same time, for the EU, with its strict data protection requirements, PNR requests by third countries (i.e. non-EU countries) create conflicts of laws. In order to resolve them, the EU concludes bilateral PNR agreements. However, the current deals, especially the one between the EU and the USA, involve a number of weaknesses. Accepting the latter, and having a pending proposal on the EU PNR system, the EU has weakened its position in negotiations with third countries. How will the EU deal with the Russian as well as with all the future requests for PNR? This paper provides legal analysis of the Russian PNR regime, pointing out common problems and giving prognosis on the global situation.

1. Introduction

Today, security experts agree that aviation security requires a risk-based, pro-active rather than reactive approach, and this is already reflected in international and national policies.[1] This strategy implies, among other things, advanced collection and analysis of personal data: since the vast majority of passengers pose no threat to civil aviation, information is critical to assess the risk. The goal is to find meaning in enormous amounts of data and then see connections and make predictions.[2]

A special role in these processes is played by Passenger Name Record (PNR).[3] PNR are used by the state authorities for security purposes, to combat terrorism and crime. Moreover, the analysis of PNR data is valuable for threat and risk assessment and management; it may help not only to identify passengers who are a known threat, but to identify potentially dangerous persons who are an unknown threat.

* Norwegian Research Center for Computers and Law (NRCCL), University of Oslo, Postboks 6706, St Olavs plass, 0130 Oslo, Norway. E-mail address: olga.enerstvedt@jus.uio.no.

[1] See, e.g. Standard 3.1.3 of ICAO's Annex 17.

[2] Schneier *Schneier on security* (2008) p. 7.

[3] PNR data will be elaborated on in Section 2.

0267-3649/$ – see front matter © 2014 Olga Mironenko Enerstvedt. Published by Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.clsr.2013.11.003

According to IATA, as of 2013, access to PNR for security purposes is required in six countries and in the works in thirty more.[4]

At the end of 2013, a Russian PNR system is planned to be implemented. All airlines operating domestic or international flights or passing Russia will have to hand over passenger data to Russian security authorities. With the largest territory in the world, the Russian Federation is a natural boundary and a natural bridge between Europe and Asia as well as one of the fastest growing markets for international air travel. Many foreign airlines, including EU airlines, carry out flights into and out of Russia[5]; in addition, around 53,000 European flights transit over Russia to Asia each year.

The key point for this paper is that usage of PNR for security purposes has a serious impact on the rights to privacy and data protection, so that these rights may be interfered with, limited or violated. Enhanced collection of passenger personal data leads to increased surveillance of mostly innocent and unsuspicious people. "Security versus privacy" has become a common expression. This dilemma generally implies balancing of these two values and definite trade-offs, usually at the price of privacy: it is obvious that security in the air must be provided, and that security, which is vital to survival, is more important than privacy. But in short, the dilemma does not necessarily imply that security needs and data protection interests cannot co-exist. Both are important for society; what is needed is to find a way to ensure both values, without loss to either. Is it possible to use PNR for security purposes and at the same time respect the passengers' rights?

Similar to other states justifying the introduction of PNR regimes, the Russian authorities explain that the new measure is warranted by the need to improve aviation security. As for the protection of passenger personal data, they state that Russia ratified the Council of Europe Convention No 108 and adopted law implementing the Convention into national law, thus, that the passengers' rights will be respected.

But despite these assurances, the EU Commission expressed concerns regarding the new Russian PNR regime. First of all, the EU became worried about the unilateral nature of the proposal. Since the EU was not familiar with the details of proposed measures and could not evaluate the impact (according to the EU officials, they raised the issue in Moscow early in 2013 and sent a letter in March, but never got a response),[6] the EU asked Russia to postpone implementation of the PNR measures and to provide additional information on the regime.[7]

Secondly, according to the EU officials, the situation with human rights in Russia creates a potential for data abuse.[8] For instance, in 2012 the EU was concerned about measures taken against members of the opposition, media freedom, the situation in the North Caucasus, the children's rights issues and issues of discrimination and racism, etc.[9] With such a background, it will undoubtedly be difficult for the EU to believe that, in contrast to the above-mentioned issues, the PNR system will respect the rights of air passengers.

Moreover, pursuant to the EU data protection legislation, transfer of PNR to Russian authorities by EU airlines will be illegal since the Russian Federation is not considered as a country providing an adequate level of data protection. Therefore, if the situation does not change, the EU airlines will find themselves in a difficult situation: to fly to or over Russia, they will need to comply with either EU or Russian law. They can either refuse to transmit the data, thereby becoming subject to Russian authorities' sanctions, or they can deliver the data in violation of the EU law.

The International Civil Aviation Organization (ICAO) Guidelines on PNR[10] stipulate in §§2.4.3-5 that air carrier must comply with the laws of the state of departure and the state destination. If the laws of the state of departure do not allow an air carrier to comply with the requirements of the state of destination, both countries should settle the conflict of laws. Prior to the settlement, states are advised to apply no fines or other sanctions against air carriers taking into account the specific circumstances of the case.

Although, in a response to the EU concerns, Russia stressed that the full text of the Order was published in September 2012 and the EU had sufficient time to prepare.[11] As a reaction, taking into account international agreements and the need for additional time for foreign and Russian carriers to prepare,[12] the term was postponed, as initially planned, from 1 July 2013 to 1 December 2013.

In 2003, when a similar problem arose for the EU carriers flying to the USA, most EU airlines chose to provide PNR to the US authorities, being unable to simply stop flying across the Atlantic.[13] However, later, this was regulated by a series of bilateral EU–US PNR agreements laying down the legal basis for the transfer. To date, the EU has such agreements with the USA, Canada and Australia. On the one hand, formally, the agreements state that they ensure an adequate level of data protection. On the other hand, data privacy advocates argue that these agreements, especially the EU–US one, fail to ensure appropriate data protection standards and contain a number of serious deficiencies and disturbing points. Clearly, compromises were made due to political and commercial needs: flights must go on. In addition, it is quite arguable whether the EU's strict data protection requirements can be achieved in the security field.

What will be the case for Russia? Will the dilemma for the EU airlines indicated above be solved, or postponed again, or

[4] IATA. Facilitation and Passenger Data http://www.iata.org/whatwedo/security/facilitation/Pages/index.aspx (data accessed: 19.08.2013).

[5] Currently, foreign air carries do not have access to the Russian domestic aviation market.

[6] Nielsen *EU tells Russia to drop air passenger data law* (2013).

[7] See Nielsen *Russia blames EU for airline data fiasco* (2013).

[8] Nielsen (2013).

[9] Council of the EU. EU Annual Report on Human Rights and Democracy in the World in 2012 (Country Reports). Brussels, 21 May 2013.

[10] Document 9944 – Guidelines on Passenger Name Record (PNR) data of 2010 (ICAO PNR Guidelines).

[11] See Nielsen (2013).

[12] The Ministry of Transport of the Russian Federation, News, 2.07.2013 http://www.mintrans.ru/news/detail.php?ELEMENT_ID=20434 (date accessed: 03.07.2013).

[13] See: Ntouvas. *Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments*. In: International Journal of Law and Information Technology. Vol. 16 (2008).