

## Passenger Name Records and data protection issues: busting some myths

*In her third post examining the overlap between data protection issues and border control (see her [first](#) and [second](#) posts) [Diana Dimitrova from KU Leuven](#) looks at the proposal for a Passenger Name Record, revived after the Charlie Hebdo attacks, from a privacy and data protection angle.*

In the past months, the Passenger Name Record (PNR) debate in the EU was revived as a response to the *Charlie Hebdo* attacks. Many arguments in defense of the EU-wide PNR proposal have been made. This post aims to clarify certain facts about PNR from a privacy, data protection and border control perspective.

### About PNR

PNR data is personal data that passengers provide to airlines when booking their flight. This data is not verified. It includes names, payment information, meal preferences, itinerary, etc. The EU PNR proposal would allow the law-enforcement authorities of the EU Member States (MS) to access this data for purposes of fighting serious crime. According to a [leaked document](#) on the envisaged changes to the proposal, the data could be stored for up to 7 days. After that it would be depersonalized and stored for 4 or 5 years. PNR is considered for flights that travel between the EU and third countries (anywhere not part of the EU), but also for intra-EU flights.

The main problems with this proposal concern the surveillance of *all* individuals traveling by plane to, from and possibly within the EU, the lack of accuracy of this data, the breach of the purpose limitation principle (i.e. re-using booking data for incompatible purposes such as law-enforcement), as well as the lack of evidence of the effectiveness, [necessity and proportionality](#) of the scheme, similar to the abolished Data Retention Directive.

### Justifying the PNR

In March 2015, [the Commission sent a letter to the European Parliament in defense of the PNR](#). The Commission tried to distinguish the proposed EU PNR from the Data Retention Directive. The latter was [struck down](#) by the Court of Justice of the European Union (CJEU) on the grounds that it represented a disproportionate interference with the rights to privacy and data protection as protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU). The Directive created a framework for storing the traffic data of all individuals. Thus, it puts everyone under surveillance, even when there is no link, direct or indirect, between the individuals whose data are saved and criminal acts.

The Commission argued that the proposed PNR represents a smaller interference with Articles 7 and 8 CFREU. Amongst the arguments put forward are that:

- (1) the PNR concerns a smaller group of individuals;
- (2) the data collected and processed do not reveal as much about an individual as phone or internet traffic data and data collection is less frequent;
- (3) passengers taking international flights are “registered for border control purposes.”

### A proportionate interference?



The CFREU is primary law. Any subsequent law, such as the PNR, must comply with its provisions, such as necessity and proportionality of the interference. Were they correctly applied to derive the arguments in (1), (2) and (3)?

The Commission argues that the PNR would concern a smaller number of individuals than the Data Retention Directive. However, the PNR could target anyone traveling to, from *and within the EU*. It could include even children, who were not affected by the Data Retention Directive. Even if the real number of affected individuals is indeed smaller, this does not mean that the surveillance it would create is targeted and proportionate, as **MEP Jan Philipp Albrecht** commented. **CEPS** has pointed out that measures such as the PNR are focused on “detection and identification of travel,” which has limited links to serious crime, e.g. the *Charlie Hebdo* attacks, the prosecution of which is PNR’s declared purpose.

The problem with the *Charlie Hebdo* case was not having to find the needle in the haystack. The perpetrators were supposedly already known to the US and French intelligent services and one of them did not actually engage in international travel to the Middle East as was suspected. Thus, the question remains whether PNR will effectively contribute to the fight against serious crime or rather disproportionately subject all international (and intra-Schengen) passengers to surveillance. The question is strengthened by the fact that there are already other means available to track transnational criminals. Thus, tracking all passengers when it might not have added value in the fight against serious crime and when there are other means available, breaches the proportionality principle and casts doubts on the respect of the essence of the rights to privacy and data protection.

Proportionality remains problematic also in argument (2), since the amount of PNR data is still huge and could be sensitive, even if it is less frequently collected. The list of data can provide a very rich picture of passengers’ private lives, including who they travel with, their travel habits, contact information, dietary requirements, payment details, etc. While it is true that this data does not reveal the same information as traffic data, it does not mean it is less intrusive *per se*. It is not clear whether all the data is needed for purposes of fighting serious crime and thus whether only the necessary data is stored and further used. While the PNR proposal suggests the masking of data after 7 days, it allows their subsequent re-personalization and thus obtaining a complete picture of someone’s travel history and other data for up to 5 years. This is clearly longer than the 2-year retention period of the Data Retention Directive. It is also questionable whether re-personalization and further data usage will be effectively controlled and overseen, e.g. by judicial authorities.

The last argument does not justify proportionality, either. There is no border control within the Schengen area. There is border control on entry and exit of the Schengen area only. Still, PNR is not meant to be used for border control purposes but to fight serious crime. Border control by current and acceding Schengen Member States is subject to the provisions of the Schengen Borders Code (SBC). The Code does not provide for the tracking of citizens enjoying the Union right to free movement (mainly EU citizens). In addition, Article 7 SBC explicitly requires that EU/EEA/CH passengers are checked against criminal law databases only on a non-systematic basis.

After the recent Germanwings crash, the **German Interior Minister** is considering introducing ID checks and exchanging passengers’ data within and outside the EU for intra-Schengen flights. This is to detect “dangerous” persons. While security is a legitimate goal, this crash was not caused due to a security breach which could have been prevented by collection and exchange of passenger data.

PNR’s interference with the rights to privacy and data protection is problematic from a proportionality perspective due to the amount of collected data and the scope of the concerned individuals. In addition, PNR is not meant for border control purposes and the two should not be mixed.



*This article gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science.*

---

May 19th, 2015 | [EU Media Policy](#), [Featured](#), [Privacy](#) | [1 Comment](#)

---

⌵

