EDITORIAL

REPEATING THE MISTAKES OF THE PAST WILL DO LITTLE GOOD FOR AIR PASSENGERS IN THE EU

The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling

Paul De Hert and Vagelis Papakonstantinou*

1. THE PROPOSED PNR DIRECTIVE AND THE UNSATISFACTORY CURRENT DATA PROTECTION FRAMEWORK

On the 17th of February an old data protection acquaintance, the EU PNR Directive[1], returned to life. On that date the Parliament's LIBE Committee released its Report[2] on its first (re-)reading of a draft that was otherwise presumed dead since 2011, when that same Committee found it unacceptable because of fundamental rights concerns and asked the Commission to withdraw it.

However, the Parliament's plenary in 2013 and the Council in 2014 decided to move forward with it[3]; such strong motivations indicate that Europeans will soon have their own PNR processing system, as the Americans have had for more than a decade.

* Paul De Hert is a Professor of EU Criminal Law at the Vrije Universiteit Brussels and at Tilburg University. Vagelis Papakonstantinou is a Post-Doctoral researcher at the Vrije Universiteit Brussels.

1 European Commission, 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, COM(2011) 32 final.

2 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report 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, 2011/0023(COD), 17.02.2015.

3 See the relevant European Parliament press release ("MEPs debate plans to use EU Passenger Name Record (PNR) data to fight terrorism"), 11.11.2014.

This resurrection[4] ought not be perceived as a joyous development for European data protection. Far from it. The Commission's original proposal of 2011 had serious data protection shortcomings arising from the fact that it ignored important understandings about the dangers of surveillance, ignored concerns about data protection requirements, and used the 2008 Police and Judicial Cooperation in Criminal Matters Framework Decision[5] as its basic data protection text of reference. However, this Framework Decision is in itself a far from sufficient[6] data protection text that is presently in the process of being replaced and is technically speaking unfit to be the framework for EU PNR processing activities.[7]

In any event, the fact remains that the general data protection environment has in the meantime substantially changed: the PNR Directive's provisions must now be reconciled with the latest case law of the Court of Justice on acceptable surveillance and with the EU data protection reform package, in particular with its draft Police and Criminal Justice Directive[8] that is to replace the 2008 Framework Decision. This applies both to substantive law and supervision model.

2. RECALLING THE PROBLEMS WITH PASSENGER DATA USED BY LAW ENFORCEMENT

PNR refer to a series of passenger details used and collected by airlines, but whose processing has come to be considered important in the global fight against terrorism. It was the Americans who first thought of using it in the law enforcement area and shortly after 9/11 imposed this 'further use' on European international flights to the US as well. Other countries followed the American example. By now the EU has entered (third generation) PNR processing agreements with the US, Australia and Canada.

---

4 Not the first in line; in fact, the PNR Directive succeeded a -failed – Commission attempt to introduce a Framework Decision in the field. See De Hert P. and Papakonstantinou V., 'The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe', *Computer Law & Security Review*, 26 (2010) 368–376.

5 Council Framework Decision 2008/977/JHA of 27 November 2008on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60, 30.12.2008.

6 See De Hert P. and Papakonstantinou V., 'The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for', *Computer Law & Security Review* 25 (2009), 403–14.

7 Even if this were not the case, it is not absolutely clear how certain provisions of this 2008 text regulating only transborder data exchanges (see Article 1.2 of the 2008 Framework Decision) may be applied at Member State level, as set by the EU PNR Directive. See Articles 11.1 and 11.2 of the draft EU PNR Directive.

8 European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012.

Only Europe is still missing a PNR processing system for its own internal air travel. The PNR Directive is the Union's approach to this end, and the need to oversee and control people who want to travel 'out' as foreign rebel fighters in the Syrian civil war is one of its supporting arguments.

It is exactly the EU approach on this matter that is disappointing. One would expect that Europeans would differentiate themselves from the US, if given the chance.

Most readers will be aware of the painful path taken to negotiate and conclude the 2003 interim US-EU PNR agreement, the 2004 US-EU Agreement, again an interim agreement this time in 2006 after the May 2006 PNR judgment of the ECJ, the 2007 US-EU agreement and the renewed 2011 US-EU agreement. Each time, reference was made to (better) data protection, and each time data protection critiques were mounted and never successfully silenced.[9]

Supposedly, Europeans would apply a better, more balanced approach to PNR processing for internal use, taking account of their data protection *acquis* this time free of American pressure to use all possible data for all possible purposes by all possible agencies. This is not the case: the recently proposed draft EU PNR Directive, similarly to the initial 2011 proposals, broadly follows the ideas found in the US-EU agreements, perhaps most notably in the breadth of the personal information collected. Does this mean that the EU legislator, after careful balancing, found no better ideas to make EU PNR processing more rights-friendly and that the US were right all along?

One should certainly hope not. A closer look at PNR processing reveals that this tool is an aggressive type of processing in the hands of law enforcement. In the enthusiastic words of the Commission,[10] law enforcement authorities may use PNR data in a number of ways: *re-actively* (in "investigations, prosecutions, unravelling of networks after a crime has been committed"), *real-time* ("use prior to the arrival or departure of passengers in order to prevent a crime, watch or arrest persons before a crime has been committed or because a crime has been or is being committed"), and *pro-actively* ("use of the data for analysis and creation of assessment criteria, which can then be used for a pre-arrival and pre-departure assessment of passengers"). The above uses pose several legal questions, ranging from legality *per se* ("watch or arrest persons *before* a crime has been committed") to the vague legal notions of "assessment criteria" and "passenger assessment" and what measures they really entail. In all of the above cases the Commission never fails to note that "in order to allow law enforcement authorities to go back sufficiently in time, a commensurate period of retention of the data by law enforcement authorities is necessary".[11]

9 See Maria Tzanou, 'The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?', (2015) 31(80), *Utrecht Journal of International and European Law* 87. See also http://itlaw.wikia.com/wiki/U.S.-EU_PNR_Arrangement.

10 See the EU PNR Directive proposal, p. 3.

11 Ibid.

3. BEHIND PNR COLLECTION IS THE DESIRE TO PROFILE THE UNKNOWN

The core of the problem is not necessarily the blacklisting, but the profiling. Only with blacklisting and profiling in mind can one understand the real controversy behind passenger data collection. Backlisting passengers may be an acceptable practice in contemporary European societies (known terrorists or criminals must not be allowed to travel, after all), however it is likely that this could be achieved by less data protection-intrusive means. For instance, the API Directive comes to mind in this regard.[12] This Directive allows the use of data regarding passenger names for border management purposes. While its limitations particularly with regard to law enforcement processing have been duly noted,[13] and could be addressed in the future, the fact remains that it collects significantly less personal data and essentially achieves the same end as the PNR Directive. Therefore, the principle of proportionality and Article 16 TFEU would definitely point in its direction, at least when pursuing passenger blacklisting purposes.

But comparing names of passengers with names on existing blacklists is only one element of the new deal. The PNR data – that is, data not only about the names of the passenger but also about the way they booked their flight tickets, the place of booking, food preferences – is wanted by law enforcement agencies to complement existing blacklists of known suspects with additional names based on passenger profiling.

Through the collection of extensive personal data on each and every passenger in the EU, PNR processing enables the preliminary assessment of each passenger's probability of being involved in or committing a crime prior to flying and/or entering a country. It goes without saying that we are dealing with a mass surveillance tool that (inevitably) reverses the presumption of innocence against passengers: each one is presumed a criminal suspect unless his or her profile hints at the opposite.

One of the problems with the EU PNR Directive is that it is silent on how profiling is done. The Directive clarifies for how long passenger data can be kept and by whom it may be kept, but the criteria for these delicate profiling operations performed on the data are not set out in the PNR Directive. In the same way, the concrete measures that law enforcement agencies are allowed to take on the basis of the results of profiling are anybody's guess.

While one should not go so far as to refuse the effectiveness of profiling for security purposes, in Europe there are rules on how to properly do it. Fundamental rights case

12 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

13 See Morren H. and Roelandt N., 'Het gebruik van Advanced Passenger Information (API) voor politionele doeleinden Een juridische en operationele analyse van het gebruik van API-data om grenstoezicht te verbeteren en illegale migratie te bestrijden', *Orde van de Dag* 2015/69.

law teaches us that all law enforcement tools need to be contained in legislation detailing their scope and nature. Data protection law imposes the use of impact assessments and other ideas contained in the EU data protection reform package[14] which are useful in mitigating data protection risks. Of particular relevance is also the recent ECJ data retention judgement[15]: while the PNR Directive, given its profiling potential, is less innocent than the data retention directive, it seems poised to make the same mistakes that led to the latter's annulment.[16] The main message of the ECJ – that after Lisbon it is no longer permitted to pass EU laws without checks and balances, assuming that Member States will add those when implementing – has clearly not been heard by the drafters of the proposed EU PNR Directive. To state this differently: if Brussels wants to make it possible for Member States to profile passenger data, it needs to say how this should be done in a foreseeable and detailed way.

4. GROWING UP IN A PROFILED WORLD

It is time for the EU to be more mature about surveillance, profiling and data mining. These techniques have been with us for some time now and we should hesitate no longer on thinking them through legally. This is future work. We know of no Member States' laws where one can find detailed regulations of these tools.

Fundamental rights force us to take up this challenge. One of the most important issues, in our opinion, is legal redress. Making decisions on profiles means accepting to make mistakes. Redress should be organised accordingly; that means it should be super-efficient. What a disappointment when one reads the proposed EU Directive. How can a passenger, that finds himself singled-out and trapped in a foreign airport, be best assisted? Adequate means of legal redress are a crucial requirement of Article 16 TFEU. In the PNR case it would mean simple rules on the competent court and on the amount of money the individual would receive if his right to data protection is infringed through unlawful processing of his or her travel data. Since a profiling system is essentially guesswork, even the establishment of an automatic compensation system in the event of mistakes would not be disproportionate. As an additional safeguard, in order to properly defend themselves individuals could be notified while at home – and not when they have landed in a foreign airport, even within the EU, where the language and legal system are inaccessible to them. Nevertheless, the draft EU PNR Directive, at least for the time being, does not provide

14 For instance, data protection by design architecture (all ideas of the draft General Data Protection Regulation of the EU data protection reform package, COM(2012)11 final, see its Articles 33 and 23 respectively).

15 *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform*, Joined Cases C-293/12 and C-594/12.

16 See Bulumac C., PNR européen: Une parodie de réponse au terrorisme, www.respect-my-privacy.eu, 28 January 2015, in particular MEP Jan Albrecht's criticism of the PNR Directive.

any practical assistance to individuals but resorts rather to the general means of redress included in the Data Protection Framework Decision,[17] the shortcomings of which were mentioned above.

The EU PNR Directive may have returned from the dead, but the world it is stepping into now is very different to that of 2011 – both from a security and from a data protection perspective. Rather than clinging to ideas and solutions from the past, its authors would do well to take the new circumstances into account, to devote some more time to creative (data protection) thinking, and to use the remaining stages of the legislative process to redraft and adapt it as best as possible.

[17] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60, 30.12.2008.