# Fundamental Rights European Experts (FREE Group)

## Opinion
## on the broader and core issues
## arising in the PNR Case currently before the CJEU
## (Case C-817/19)

by

**Douwe Korff**
*Emeritus Professor of International Law, London Metropolitan University*
*Associate, Oxford Martin School, University of Oxford*

### === EXECUTIVE SUMMARY ===

(with a one-page "at a glance" overview of the main findings and conclusions)

November 2021

# Fundamental Rights Europe Experts (FREE Group)

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

**About the FREE Group:**

The Fundamental Rights European Experts Group (FREE Group) is a Belgian non-governmental organisation (*Association Sans But Lucratif*, ASBL), registered at Belgian Moniteur: Number 304811.

According to art 3 and 4 of its Statute, the association focus is on monitoring, teaching and advocating in the European Union freedom security and justice related policies. In the same framework it also follows the EU actions in protecting and promoting EU values and fundamental rights in the Member States as required by the article 2, 6 and 7 of the Treaty on the European Union (risk of violation by a Member State of EU founding values).

https://free-group.eu/free-group-members/

**About the author:**

Douwe Korff is a Dutch comparative and international lawyer specialising in human rights and data protection. He is emeritus professor of international law at London Metropolitan University and visiting professor at the universities of Zagreb and Rijeka in Croatia; an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin.

Douwe Korff has carried out many studies relating to data protection for the EU, the Council of Europe, the UN (ITU), the British Commonwealth, and UK authorities.

**Acknowledgments:**

The author wishes to acknowledge that in preparing this paper he has drawn on the work of other FREE Group members including Emilio de Capitani and Christian Thönnes. He is also grateful for helpful comments from Kristina Irion, co-author of the recent evaluation report on the Dutch PNR Law.

# Fundamental Rights Europe Experts (FREE Group)

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

## Main findings and conclusions at a glance

In my opinion, the appropriate tests to be applied to mass surveillance measures such as are carried out under the PNR Directive (and were carried out under the Data Retention Directive, and are still carried out under the national data retention laws of the EU Member States that continue to apply in spite of the CJEU case-law) are:

**Have the entities that apply the mass surveillance measure – i.e., in the case of the PNR Directive (and the DRD), the European Commission and the EU Member States – produced reliable, verifiable evidence:**

**(i)** **that those measures have actually, demonstrably contributed significantly to the stated purpose of the measures, i.e., in relation to the PNR Directive, to the fight against PNR-relevant crimes (and in relation the DRD, to the fight against "serious crime as defined by national law"); and**

**(ii)** **that those measures have demonstrably not seriously negatively affected the interests and fundamental rights of the persons to whom they were applied?**

If the mass surveillance measures do not demonstrably pass both these tests, they are fundamentally incompatible with European human rights and fundamental rights law and the Charter of Fundamental Rights; this means the measures must be justified, by the entities that apply them, on the basis of hard, verifiable, peer-reviewable data.

The conclusion reached by the European Commission and Dutch Minister of Justice: that overall, the PNR Directive, respectively the Dutch PNR law, had been "effective" because the EU Member States said so (Commission) or because PNR data were quite widely used and the competent authorities said so (Dutch Minister) is fundamentally flawed, given that this conclusion was reached in the absence of any real supporting data. Rather, my analyses show that:

- Full PNR data are disproportionate to the purpose of basic identity checks;
- The necessity of the PNR checks against Interpol's Stolen and Lost Travel Document database is questionable;
- The matches against unspecified national databases and "repositories" are not based on foreseeable legal rules and are therefore not based on "law";
- The necessity and proportionality of matches against various simple, supposedly "suspicious" elements (tickets bought from a "suspicious" travel agent; "suspicious" travel route; etc.) is highly questionable; and
- The matches against more complex "pre-determined criteria" and profiles are inherently and irredeemably flawed and lead to tens, perhaps hundreds of thousands of innocent travellers wrongly being labelled to be a person who "may be" involved in terrorism or serious crime, and are therefore unsuited (D: *ungeeignet*) to the purpose of fighting terrorism and serious crime.

**The hope must be that the Court will stand up for the rights of individuals, enforce the Charter of Fundamental Rights, and declare the PNR Directive (like the Data Retention Directive) to be fundamentally in breach of the Charter.**

- o – O – o –

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

# Executive Summary

This document summarises the analyses and findings in the full Opinion on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19), using the same headings and heading numbers. Please see the full opinion for the full analyses and extensive references. A one-page "at a glance" overview of the main findings and conclusions is also provided.

The opinion drew in particular on the following three documents, also mentioned in this Executive Summary:

- Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2020) 305 final, 24 July 2020 (hereafter: "**Commission report**"), available at: https://op.europa.eu/en/publication-detail/-/publication/4bfd0de3-cda3-11ea-adf7-01aa75ed71a1/language-en
- Commission Staff Working Document accompanying the above Commission Report, SWD(2020) 128 final, 24 July 2020 (hereafter: "**Staff working document**"), available at: https://op.europa.eu/en/publication-detail/-/publication/9c419b94-cda3-11ea-adf7-01aa75ed71a1/language-en/format-PDF/source-search
- Evaluatie PNR-Wet (**Evaluation of the Dutch PNR Law**), October 2021, carried out under Article 25 of the Dutch PNR Law and presented to the First Chamber of the Dutch Parliament on 12 November 2021, available at: https://www.eerstekamer.nl/overig/20211112/evaluatie_pnr_wet_wodc_oktober/document (in Dutch; relevant passages are translated into English in the full opinion)

- o – O – o -

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

## 1. Introduction

In the opinion, after explaining, at 2, the broader context in which personal data are being processed under the PNR Directive, I try to assess whether the processing that the PNR Directive requires or allows is suitable, effective and proportionate to the aims of the directive. In doing so, in making those assessments, I base myself on the relevant European human rights and data protection standards, summarised at 3.

NB: The opinion focusses on the system as it is designed and intended to operate, and on what it allows (even if not everything that may be allowed is [yet] implemented in all Member States), and less on the somewhat slow implementation of the directive in the Member States and on the technical aspects that the Commission report and the staff working document often focussed on. It notes in particular a number of elements or aspects of the directive and the system it establishes that are problematic, either conceptually or in the way they are supposed to operate or to be evaluated.

## 2. PNR in context

In the footsteps of the US and UK intelligence services (as revealed by Snowden), the EU Member States' law enforcement agencies are increasingly using their access to bulk data – bulk e-communications data, financial data, PNR data, etc. – to "mine" the big data sets by means of sophisticated, self-learning algorithms and Artificial Intelligence (AI).

The European Union Agency for Law Enforcement Cooperation, Europol, has become increasingly involved in algorithm/AI-based data analysis (or at least in the research underpinning those technologies), and last year the Commission proposed to significantly further expand this role.

The processing of PNR data under the PNR Directive must be seen in these wider contexts: the clear and strengthening trend towards more "proactive", "preventive" policing by means of analyses and algorithm/AI-based data mining of (especially) large private-sector data sets and databases; the increasingly central role played by Europol in this (and the proposal to expand that role yet further); the focusing on "persons of interest" against whom there is (as yet) insufficient evidence for action under the criminal law (including, in relation to Europol, persons against whom there is an "Article 36 alert" in its SIS II database); and the still increasing intertwining of law enforcement and national security "intelligence" operations in those regards.

**Notably, "Article 36 SIS alerts" have been increasing, and in the Netherlands, in 2020, 82.4% of all PNR "hits" against the Schengen Information System, confirmed by the Dutch Passenger Information Unit established under the PNR Directive, were "hits" against "Article 36 alerts".**

Human rights-, digital rights- and broader civil society NGOs have strongly criticised these developments and warned of the serious negative consequences. Those concerns should be taken seriously, and be properly responded to.

## 3. Legal standards

General fundamental rights standards stipulate that all interferences with fundamental rights must be based on a "law" that meets the European "quality of law" standards: the law must be public, clear and specific, and foreseeable in its application; the interferences must be limited to what is "necessary" and "proportionate" to serve a "legitimate aim" in a democratic society; the relevant limitations must be set out in the law itself (and not left to the discretion of states or state authorities); and those affected by the interferences must be able to challenge them and have a remedy in a court of law. Generalised, indiscriminate surveillance of whole populations (such as all air passengers flying to or from the EU) violates the EU Charter of Fundamental Rights. A special exception to this prohibition accepted by the EU Court of Justice in the *La Quadrature du Net* case, which allows EU Member States to respond to "serious", "genuine and present or foreseeable" threats to "the essential functions of the State and the fundamental interests of society" must be strictly limited in time and place: it cannot form the basis for continuous surveillance of large populations (such as all air passengers) generally, on a continuous, indefinite basis: that would turn the (exceptional) exception into the rule. Yet that is precisely what the PNR Directive provides for.

European data protection law expands on the above general principles in relation to the processing of personal data. The (strict) case-law of the CJEU and the European Court of Human Rights on data protection generally and generalised surveillance in particular are reflected in the European Data Protection Board's European Essential Guarantees for surveillance (EEGs).

Processing of information on a person suggesting that that person "may be" involved in criminal activities is subject to especially strict tests of legitimacy, necessity and proportionality.

**Contrary to assertions by the European Commission and representatives of EU Member States (*inter alia*, at the hearing in the PNR case in July 2021) that the processing under the PNR Directive has little or no effect on the rights and interests of the data subjects, the processing under the directive must under EU data protection law be classified as posing "high risks" to the fundamental rights and interests of hundreds of millions of airline passengers.**

Under the Law Enforcement Directive (as under the GDPR), this means that the processing should be subject to careful evaluation of the risks and the taking of remedial action to prevent, as far as possible, any negative consequences of the processing – such as the creation of "false positives" (cases in which a person is wrongly labelled to be a person who "may be" involved in terrorism or serious crime). It also means that if it is not possible to avoid excessive negative consequences, the processing is "not fit for purpose" and should not be used.

Under the proposed Artificial Intelligence Act that is currently under consideration, similar duties of assessment and remedial action – or abandoning of systems – are to apply to AI-based processes.

# 4. The PNR Directive

## 4.1 Introduction

## 4.2 The system

Under the PNR Directive, special "Passenger Information Units" (PIUs) in each EU Member State match the data contained in so-called passenger name records (PNRs) that airlines flying into or from the EU have to provide to those units against supposedly relevant lists and databases, to both identify already "known" formally wanted persons or already "known" "persons of interest" who "may be" involved in terrorism or other serious crime, and to "identify" (i.e., label) previously "unknown" persons who "may be" involved in such activities by means of "risk analyses" and the identification of "patterns" and "profiles" based on the identified patterns (see below, at 4.7).

The opinion analyses and assesses all major elements of the system in turn.

## 4.3 The aims of the PNR Directive

In simple terms, the overall aim of the PNR Directive is to facilitate the apprehension of terrorists and individuals who are involved in terrorism or other serious transnational crime, including in particular international drug- and people trafficking.

However, the first aim of the checking of the PNR data by the PIUs is more limited than the aims of the directive overall; this is:

> to identify persons who require further examination by the competent authorities [see below, at 4.5], and, where relevant, by Europol [see below, at 4.11], in view of the fact [?] that such persons may be involved in a terrorist offence or serious crime. (Article 6(1)(a))

When there is a match of PNR data against various lists, i.e., a "hit" (see below, at 4.9), the PNR passes this "hit" on to certain "competent authorities" (see below, at 4.5) for "further examination"; if the initial "hit" was generated by automated means, this is only done after a manual review by PIU staff. In practice, about 80% of initial "hits" are discarded (see below, at 4.9).

**It is one of the main points of the opinion that the suitability, effectiveness and proportionality of the PNR Directive cannot and should not be assessed by reference to the number of initial "hits" noted by the PIUs, compared to the number of cases passed on for "further examination" to the competent authorities, but rather, with reference to more concrete outcomes (as is done in section 5.2).**

## 4.4 The legal bases for the PNR Directive

It appears obvious from the Court of Justice opinion on the Draft EU-Canada Agreement that the PNR Directive, like that draft agreement, should have been based on Articles 16 and 87(2)(a) TFEU, and not on Article 82(1) TFEU. It follows that the PNR Directive, too, appears to not have been adopted in accordance with the properly applicable procedure. That could lead to the directive being declared invalid on that ground alone.

### 4.5 The competent authorities

Although most competent authorities (authorities authorised to receive PNR data and the results of processing of PNR data from the PIUs) in the EU Member States are law enforcement agencies, "**many Member States [have designated] intelligence services, including military intelligence services, as authorities competent to receive and request PNR data from the Passenger Information Unit**", and "**in some Member States the PIUs are actually "embedded in … [the] state security agenc[ies]**".

**Given the increasingly close cooperation between law enforcement agencies (and border agencies) and intelligence agencies, in particular in relation to the mining of large data sets and the development of evermore sophisticated AI-based data mining technologies by the agencies working together (and in future especially also with and through Europol), this involvement of the intelligence agencies (and in future, Europol) in PNR data mining must be seen as a matter of major concern.**

### 4.6 The crimes covered ("PNR-relevant offences")

The PNR Directive stipulates that PNR data and the results of processing of PNR data may only be used for a range of terrorist and other serious offences, as defined in Directive 2017/541 and in an annex to the PNR Directive, respectively (so-called "**PNR-relevant offences**").

**However, the definitions and lists of PNR-relevant offences are vague and open-ended, and to a large extent left to the EU Member States – which means that the application of the directive in practice is not foreseeable, which in turn raises serious doubts as to whether it constitutes "law" in the European sense. That vagueness also makes it difficult to assess the suitability, effectiveness or proportionality of the directive.**

### 4.7 The categories of data subjects targeted and the meaning of (confirmed) "hits"

The PNR Directive covers all the approximately **one billion (!) PNRs** on all passengers on all extra-EU flights and almost all passengers on intra-EU flights each year, covering (at a conservative guess) some **500 million individuals**.

The processing under the PNR Directive aims to single out quite different categories of data subjects from this large base: on the one hand, it seeks to identify already **"known" formally wanted persons** (i.e., persons formally designated suspects under criminal [procedure] law, persons formally charged with or indicted for, or indeed already convicted of PNR-relevant offences) and already **"known" "persons of interest"** (but who are not yet formally wanted) by checking basic identity data in the PNRs against the corresponding data in "wanted" lists (such as "Article 26 alerts" in SIS II); and on the other hand, it seeks to "identify" **previously "unknown" persons** as possibly being terrorist or serious criminals, or "of interest", on the basis of vague indications and probability scores. In the latter case, the term "identifying" means no more than labelling a person as a possible suspect or "person of interest" on the basis of a probability.

**The opinion argues that any assessment of the suitability, effectiveness and proportionality of the processing must make a fundamental distinction between these different categories of data subjects (as is done in section 5).**

### 4.8 The categories of personal data processed

An annex to the PNR Directive lists the specific categories of data that airlines must send to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart. This obligation is stipulated with regard to extra-EU flights but can be extended by each Member State to apply also to intra-EU flights – and all but one Member States have done so. **The list of PNR data is much longer than the Advance Passenger Information (API) data that airlines must already send to the Member States under the API Directive**, and includes information on ***travel agents*** used, ***travel routes***, ***email addresses***, ***payment (card) details***, ***luggage***, and ***fellow travellers***. On the other hand, ***often some basic details (such as date of birth) are not included in the APIs***.

#### The use of sensitive data

**The PNR Directive prohibits the processing of sensitive data**, i.e., "data revealing a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation". In the event that PNR data revealing such information are received by a PIU, they must be deleted immediately. Moreover, competent authorities may not take "any decision that produces an adverse legal effect on a person or significantly affects a person" on the basis of such data.

**However, PNR data can be matched against national lists and data "repositories" that may well contain sensitive data. Moreover, as noted at 4.9(f), below, the provisions in the PNR Directive do not really protect against discriminatory outcomes of the profiling that it encourages.**

### 4.9 The different kinds of matches

#### (a) Matching of basic identity data in PNRs against the identity data of "known" formally wanted persons

PNR data are matched against SIS II alerts on "known" formally wanted persons (including "Article 26 alerts") and against "relevant" national lists of "known" formally wanted persons. This is usually done by automated means, followed by a manual review. The Commission reports that approximately 81% of all initial matches are rejected – and not passed on to competent authorities for further examination. Notably:

- **the quality of the PNR data as received by the PIUs, including even of the basic identity data, is apparently terrible and often "limited"**; this is almost certainly the reason for the vast majority of the 81% rejections;

- **most of the long lists of PNR data are not needed for basic identity checks**: full names, date of birth, gender and citizenship/nationality should suffice – and a passport or identity card number would make the match more reliable still. All those data are included in

the API data, and all are included in optical character recognition format in the machine-readable travel documents (MRTD) that have been in wide use since the 1980s.

**In other words, paradoxically, PNR data are both excessive for the purpose of basic identity checks (by containing extensive data that are not needed for such checks), and insufficient ("too limited"), in particular in relation to intra-Schengen flights (by not [always] including the dates of birth of the passengers).**

- the lists against which the PNR data are compared, including in particular the SIS alerts and the EAW lists, but also many national lists, relate to many more crimes than are subject to the PNR Directive ("PNR-relevant offences") – but **in several Member States "hits" against not-PNR-relevant suspects (etc.) are still passed on to competent authorities, in clear breach of the purpose-limitation principle underpinning the directive**.

In that respect, it should be noted that the Commission staff working document claims that in relation to situations in which the PNR data is "too limited" (typically, by not including date of birth), *"[t]he individual manual review provided for in Article 6.5 of the PNR Directive protects individuals against the adverse impact of potential 'false positives'"* – but this is **simply untrue**:

**While a confirmed matching of identity data in relation to a person who is formally wanted in relation to PNR-relevant offences can be regarded as a "positive" result of the identity check, a "hit" in relation to a person who is wanted for not-PNR-relevant offences should of course not be regarded as a positive result under the PNR Directive.**

### (b) Matching of basic identity data in PNRs against the identity data of "known" "persons of interest"

In principle, the matching of basic identity data from PNRs against lists of basic identity data of "persons of interest" listed in the SIS system (and comparable categories in national law enforcement repositories), like the matching of data on formally wanted persons, should be fairly straight-forward. However, the PNRs in this regard first of all suffer from the same two deficiencies as were discussed in relation to matches for formally wanted persons, discussed at (a), above: PNR data are both excessive for the purpose of basic identity checks (by containing extensive data that are not needed for such checks), and insufficient ("too limited"), in particular in relation to intra-Schengen flights (by not [always] including the dates of birth of the passengers). The third issue identified in the previous sub-section, that SIS alerts (and similar alerts in national law enforcement repositories) can relate to many more criminal offences than those that are "PNR-relevant" also applies: many persons labelled "person of interest" will be so labelled in relation to "non-PNR-relevant" offences.

**In my opinion, while a confirmed matching of identity data in relation to persons who are formally wanted in relation to (formally suspected of, charged with, or convicted of) PNR-relevant offences can be regarded as a "positive" result of an identity check, *a "hit" in relation to persons who are labelled "person of interest" should not be regarded as a positive result under the PNR Directive – certainly of course not if they are so labelled in***

***relation to non-PNR-relevant offences, but also not if they are in no way implicated as in any way being culpable of PNR-relevant offences.***

**In my opinion,** ***even confirmed "hits" confirming the identity of already listed "persons of interest" should not be regarded as "positive" results under the PNR Directive unless they result in those persons subsequently being formally declared to be formal suspects in relation to terrorist or other serious, PNR-relevant criminal offences*****.**

### (c) Matching of PNR Data against data on lost/stolen/fake credit cards and lost/stolen/fake identity or travel documents

The staff working document makes clear that PNR data are checked by "a large majority of PIUs" against **Interpol's Stolen and Lost Travel Document database** as one "relevant database". However, this is somewhat of a residual check because that database is also already made available to airlines through Interpol's "**I-Checkit**" facility. Moreover:

**Even leaving the issue of purpose-limitation aside, a "hit" against a listed lost/stolen/fake credit card or a lost/stolen/fake identity or travel document should still only be considered a "positive result" in terms of the PNR Directive if it results in a person subsequently being formally declared to be (at least) a formal suspect in relation to terrorist or other serious, PNR-relevant criminal offences.**

### (d) Matching of PNR data against other, unspecified, supposedly relevant (in particular national) databases

It is far from clear what databases can be – and in practice, in the different Member States, what databases actually are – regarded as "relevant databases" in terms of the PNR Directive: this is left to the Member States. At the July 2021 Court hearing, the representative of the Commission said that the data of *Facebook*, *Amazon* and *Google* could not be regarded as "relevant", and that law enforcement databases (*des bases policières*) would be the most obvious "relevant" databases. But the Commission did not exclude matches against other databases with relatively "hard" data, such as databases with financial data (credit card data?) or telecommunications data (location data?).

**The vagueness of the phrase "relevant databases" in Article 6(3)(a) and the apparently wide discretion granted to Member States to allow matching against all sorts of unspecified data sets is incompatible with the Charter of Fundamental Rights and the European Convention on Human Rights. It means that the application of the law is not clear or foreseeable to those affected – i.e., the provision is not "law" in the sense of the Charter and the Convention (and EU law generally) – and that the laws can be applied in a disproportionate manner.**

***In other words, even in relation to the basic checks on the basis of lists of "simple selectors", the PNR Directive does not ensure that those checks are based on clear, precise, and in their application foreseeable Member State laws, or that those laws are only applied in a proportionate manner. In the terminology of the European Court of Human Rights, the directive does not protect individuals against arbitrary interferences with the rights to privacy and protection of personal data.***

### (e) Matching of PNR data against lists of "suspicious travel agents", "suspicious routes", etc.

The staff working document repeatedly refers to checks of PNR data against "patterns" such as tickets being bought from "suspicious" travel agents; the use of "suspicious" travel routes; passengers carrying "suspicious" amounts of luggage (and the Dutch evaluation report even mentions that a person wearing a suit and hastening through customs [while being black] was regarded by custom authorities as fitting a "suspicious" pattern).

**No proper prosecuting or judicial authority could declare travellers to be a formal suspect – let alone to charge, prosecute or convict a traveller – on the basis of a match against such simple "suspicious" elements alone.** In my opinion:

**For the purpose of evaluating the suitability, effectiveness and proportionality of the PNR Directive (and of the practices under the directive), a simple "hit" against these vague and far-from-conclusive factors or "criteria" should not be regarded as a "positive" result.**

**Rather, a "hit" against such vague "criteria" as the purchase of an air ticket from a "suspicious" travel agent, or the using of a "suspicious" route, or the carrying of a "suspicious" amount of luggage – let alone "walking fast in a suit (while being black)" – should again only be considered a "positive result" in terms of the PNR Directive if it result in a person subsequently being formally declared to be (at least) a formal suspect in relation to terrorist or other serious, PNR-relevant criminal offences.**

### (f) Matching of data in the PNRs against more complex "pre-determined criteria" or profiles

### (fa) Introduction

Under the PNR Directive, PIUs may, in the course of carrying out their assessment of whether passengers "may be involved in a terrorist offence or [other] serious crime", "process PNR data against pre-determined criteria". As also noted by the EDPS, it is clear that **the PNR data can be matched against "patterns" discerned in previous data and against "profiles" of possible terrorists and serious criminals created on the basis of these patterns, that are more complex than the simple patterns discussed at (e), above.** This is also undoubtedly the direction in which searches for terrorists and other serious criminals are moving.

### (fb) The nature of the "pre-determined criteria"/"profiles"

The EU and EU Member State agencies are increasingly applying, or are poised to apply, increasingly sophisticated data mining technologies such as are already used by the UK (and US) agencies. This involves **self-learning, AI-based algorithms** that are constantly dynamically re-generated and refined through loops linking back to earlier analyses. The software creates **constantly self-improving and refining profiles** against which it matches the massive amounts of data – and in the end, **it produces lists of individuals that the algorithm suggests may (possibly or probably) be terrorists, or associates of terrorists or other serious criminals**. It is the stated policy of the EU to accelerate the development and deployment of these sophisticated technologies, under the guidance of Europol.

**Whatever the current level of use of such sophisticated techniques in law enforcement and national security contexts in the Member States (as discussed at (fd), below), if the PNR Directive is upheld as valid in its current terms, nothing will stand in the way of the ever-greater deployment of these more sophisticated (but flawed) technologies in relation to air passengers. That would also pave the way to yet further use of such (dangerous) data mining and profiling in relation to other large population sets (such as all users of electronic communications, or of bank cards).**

### (fc) The creation of the "pre-determined criteria"/"profiles"

**Given (a) the increasingly sophisticated surveillance and data analysis/data mining/risk assessment technologies developed by the intelligence services of the EU Member States (often drawing on US and UK experience) and now also by law enforcement agencies and (b) the clear role assigned to Europol in this respect, it would appear clear that there is being developed a *cadre* of data mining specialists in the EU – and that the PNR data are one of the focus areas for this work.**

**In other words, the "pre-determined criteria" – or AI-based algorithms – that are to be used in the mining of the PNR data are being developed, not solely by or within the PIUs but by this broader *cadre* that draws in particular on intelligence experts (some of whom may be embedded in the PIUs). *The PNR databases are (also) between them a test laboratory for data mining/profiling technologies.***

**And (c) there is nothing in the PNR Directive that stands in the way of using other data than PNR data in the creation of "pre-determined criteria", or indeed in the way of using profiles developed by other agencies (including intelligence agencies) as "pre-determined criteria" in the PIU analyses.**

### (fd) The application of the more complex "pre-determined criteria"/"profiles" in practice

It would appear that to date, few Member States are as yet using data mining in relation to PNR data in as sophisticated a way as described in sub-section (fb), above (or at least acknowledge such uses).

However, in a range of EU Member States algorithm/AI-based profiling is already in use in relation to broader law enforcement (and especially crime prevention). Moreover, the aim of the Commission and the Member States is expressly to significantly expand this use, with the help of Europol and its Travel Intelligence Task Force, and through "*training on the development of pre-determined criteria*" in "*an ongoing EU-funded project, financed under the ISF-Police Union Actions*."

**This merely underlines the point I made in the previous sub-sections: that the PNR database is being used as a test laboratory for advanced data mining technologies, and that if the PNR Directive is upheld as valid in its current terms, nothing will stand in the way of the**

**ever-greater deployment of these more sophisticated (but flawed) technologies in relation to air passengers, and others.**

***The fact that sophisticated data mining and profiling is said to not yet be in widespread operational use in most Member States should not be a reason for ignoring this issue – on the contrary: this is the desired destination of the analyses.***

### (fe) The limitations of and flaws in the technologies

There are three main problems with algorithmic data mining-based detection of rare phenomena (such as terrorists and serious criminals in a general population):

- **The base-rate fallacy and its effect on false positives:**

**In very simple layperson's terms, the base-rate fallacy means that if you are looking for very rare instances or phenomena in a very large dataset, you will inevitably obtain a very high percentage of false positives in particular – and *this cannot be remedied by adding more or somehow "better" data: by adding hay to a haystack*.**

As noted above, at 4.7, a very rough guess would be that on average the 1 billion people counted by Eurostat as flying to or from the EU relate to 500 million distinct individuals. In other words, **the base rate for PNR data can be reasonably assumed to be in the region of 500 million**.

The Commission reports that there are initial "hits" in relation to 0.59% of all PNRs, while 0.11% of all PNRs are passed on as confirmed "hits" to competent authorities for "further examination".

**The Commission report and the staff working document appear to imply – and certainly do nothing to refute – that the 0.11% of all confirmed "hits" that are passed on to competent authorities are all "true positives". However, that glaringly fails to take account of the base rate, and its impact on results.**

Even if the PNR checks had a failure rate of just 0.1% (meaning that (1) in relation to persons who are actually terrorists or serious criminals, the PIUs will rightly confirm this as a proper "hit" 99.9% of the time, and fail to do so 0.1% of the time and (2) in relation to persons who are not terrorists, the PIUs will rightly not generate a confirmed "hit" 99.9% of the time, but wrongly register the innocent person as a confirmed "hit" 0.1% of the time) the probability that a person flagged by this system is actually a terrorist would still be closer to 1% than to 99%.

**In any case, even if the accuracy rate of the PNR checks were to be as high as this assumed 99.9% (which of course is unrealistic), that would still lead to some 500,000 false positives each year.**

*Yet the Commission documentation is silent about this.*

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

- **Built-in biases:**

The Commission staff working document claims that, because the "pre-determined criteria" that are used in algorithmic profiling may not be based on sensitive data, "*the assessment cannot be carried out in a discriminatory manner*" and that "*[t]his limits the risk that discriminatory profiling will be carried out by the authorities*." **This is simply wrong**.

**In simple terms: since "*intimate part[s] of [a person's] private life*" can be deduced, or at least inferred, from seemingly innocuous information – such as data included in PNRs (in particular if matched against other data) – those "*intimate aspects*" are not "*fully protected by the processing operations provided for in the PNR Directive*".**

Indeed, in a way, the claim to the contrary is absurd: the whole point of "risk analysis" based on "pre-determined criteria" is to discover unknown, indeed hidden matters about the individuals who are being profiled: inferring from the data on those people, on the basis of the application of those criteria, that they are persons who "may be" involved in terrorism or other serious crimes surely is a deduction of an "intimate aspect" of those persons (even if it is not specifically or necessarily a sensitive datum in the GDPR sense – although if the inference was that a person "might be" an Islamist terrorist, that would be a [tentatively] sensitive datum in the strict sense).

**Moreover, even without specifically using or revealing sensitive information, the outcomes of algorithmic analyses and processing, and the application of "abstract", algorithm/AI-based criteria to "real" people can still lead to discrimination.**

The PNR Directive stipulates that **the assessment[s] of passengers prior to their scheduled arrival in or departure from the Member State** carried out with the aim of identifying persons who require further examination by the competent authorities of the directive "***shall be carried out in a non-discriminatory manner***".

However, this falls considerably short of stipulating: (i) that the "pre-determined criteria" (the outputs of the algorithms) are not biased in some way and (ii) that measures must be taken to ensure that the outcomes of the assessments are not discriminatory. It is important to address both those issues (as explained in a recent EDRi/TU Delft report).

Given that **profile-based matches to detect terrorists and other serious criminals are inherently "high risk"** (as noted at 3, above and further discussed at 5, below), it requires an in-depth **Data Protection Impact Assessment** under EU data protection law, and indeed a broader **human rights impact assessment**. The need for serious pre-evaluation of algorithms to be used in data mining and for continuous re-evaluation throughout their use is also stressed in various paragraphs in the recent Council of Europe recommendation on profiling. The proposed AI Act also requires this. However, **no serious efforts have been made by the European Commission or the EU Member States to fulfil these duties**. Neither have ensured that full, appropriate basic information required for such serious *ex ante* and *ex post* evaluations is even sought or recorded.

**Opinion**
**on the broader and core issues arising in the PNR Case currently before the CJEU (Case C-817/19)**
**=== EXECUTIVE SUMMARY ===**
**by Douwe Korff**

**In sum: the European Commission and the EU Member States have not ensured that in practice the processing of the PNR data, and the linking of those data to other data (databases and lists), does not have discriminatory outcomes. The mere stipulation that outputs of algorithmic/AI-based profiling should not be "solely based on" sensitive aspects of the data subjects (the airline passengers) falls far short of ensuring compliance with the prohibition of discrimination.**

- **Opacity and unchallengeability of decisions:**

In the more developed "artificial intelligence" or "expert" systems, the computers operating the relevant programmes create feedback loops that continuously improve the underlying algorithms – with almost no-one in the end being able to explain the results: the analyses are based on underlying code that cannot be properly understood by many who rely on them, or even expressed in plain language. This makes it extremely difficult to provide for serious accountability in relation to, and redress against, algorithm-based decisions generally.

**Profiling thus poses a serious threat of a Kafkaesque world in which powerful agencies take decisions that significantly affect individuals, without those decision-makers being able or willing to explain the underlying reasoning for those decisions, and in which those subjects are denied any effective individual or collective remedies.**

**That is how serious the issue of profiling is: it poses a fundamental threat to the most basic principles of the Rule of Law and the relationship between the powerful and the people in a democratic society.**

Specifically in relation to PNR:

- **PIU staff cannot challenge algorithm-based computer outputs;**
- **The staff of the competent authorities are also unlikely (or indeed also effectively unable) to challenge the computer output;** and
- **Supervisory bodies cannot properly assess the systems.** External supervisory bodies such as Member States' data protection supervisory authorities will generally not be given access to the underlying data, cannot review the algorithms at the design stage or at regular intervals after deployment and in any case do not have the expertise. Internal bodies are unlikely to be critical and may involve the very people who design the system (who write the code that provides the [dynamic] algorithm). The report on the evaluation of the Dutch PNR Law noted that under that law (under which the algorithms/profiles are supposed to be checked by a special commission):

  > **The rules [on the creation of the pre-determined criteria] do not require the weighing [of the elements] or the threshold value [for regarding a "hit" against those criteria to be a valid one] to meet objective scientific standards.**

**This is quite an astonishing matter. It acknowledges that the algorithm/AI-based profiles are essentially unscientific. In my opinion, this fatally undermines the way the pre-determined criteria are created and "tested" in the Netherlands. Yet at the same time, the Dutch system, with this "special commission", is probably better than what is in place in most other EU Member States. This surely is a matter that should be taken into account in any assessment of the PNR system EU-wide – including the assessment that is shortly to be made by the Luxembourg Court.**

**In sum:**

- **because the "base-rate" for the PNR data mining is so high (in the region of 500 million people) and the incidence of terrorists and serious criminals within this population so relatively low, algorithm/AI-based profiling is likely to result in tens of thousands of "false positives": individual air passengers who are wrongly labelled to a be person who "may be" involved in terrorism or other serious crime;**
- **the provisions in the PNR Directive that stipulate that no sensitive data may be processed, and that individual decisions and matches may not be "solely based on" sensitive aspects of the individuals concerned do not protect those individuals from discriminatory outcomes of the profiling;**
- **the algorithm/AI-based outcomes of the processing are almost impossible to challenge because those algorithms are constantly dynamically changed ("improved" through self-learning) and therefore in effect impossible to fully comprehend even by those carrying out the analyses/risk assessments; and**
- **the outputs and outcomes of the algorithm/AI-based profiling and data mining and matching are not subject to proper scientific testing or auditing, and extremely unlikely to made subject to such testing and auditing.**

### 4.10 Direct access to PNR data by EU Member States' intelligence agencies

It appears that at least in the Netherlands, the national intelligence agencies are granted direct access to the bulk PNR database, without having to go through the PIU (or at least without this being properly recorded).

If the Dutch authorities were to argue that such direct access to data by the Dutch intelligence agencies is outside EU law, they would be wrong. Specifically, in its *LQDN* judgment, the CJEU held that the rules on personal data processing operations by entities that are, in that processing, subject to EU data protection law (in that case, providers of electronic communication services, who are subject to the e-Privacy Directive), including processing operations by such entities resulting from obligations imposed on them (under the law) by Member States' public authorities (in that case, for national security purposes) can be assessed for their compatibility with the relevant EU data protection instrument and the Charter of Fundamental Rights.

**In my opinion, if the Dutch intelligence and security agencies do indeed have direct access to the PNR database, without having to go through the Dutch PIU (the Pi-NL), or without that being recorded – as appears to be pretty obviously the case – that is in direct breach of the PNR Directive, of the EU data protection instruments, and of the EU Charter of Fundamental Rights.**

Whether the EU data protection instruments and the PNR Directive are similarly circumvented in other EU Member States, I do not know. Let me just recall that in several Member States, the PIU is "embedded in … [the] state security agenc[ies]". However, the Dutch example shows how dangerous, in a democratic society, the accruing of such bulk databases is.

### 4.11 Dissemination and subsequent use of the data and purpose-limitation

#### (a) Spontaneous provision of PNR data and information on (confirmed) "hits"

**In principle, subject only to a "relevant and necessary" requirement in relation to transmissions to the other PIUs, confirmed "hits" can be very widely shared across all the EU Member States, both between the PIUs but also, via the PIUs, with any "competent authority" in any Member State (including intelligence agencies where those are designated as such: see at 4.5, above).**

#### (aa) Spontaneous provision of information to domestic competent authorities on the basis of matches against lists and databases (including SIS II)

The Commission staff working report gives no insight into the actual scope of spontaneous dissemination of PNR data or "results of the processing" of PNR data by the PIUs on the basis of (confirmed) "hits" to competent authorities in the PIUs' own countries. The report on the evaluation of the Dutch PNR Law suggests that, in that country, spontaneous provisions of PNR to Dutch authorities "for further examination" are still effectively limited to (confirmed) matches against the SIS II database, and indeed to matches against the alerts listed in Articles 26 and 36 of the Council Decision establishing that database (respectively, alerts for persons wanted for arrest for extradition, and alerts relating to people or vehicles requiring discreet checks). The Dutch SIS II matches amounted to roughly 10 in every 100,000 passengers (2:100,000 "Article 26" matches and 8:100,000 "Article 36" matches).

**If the Dutch statistics of 10:100,000 and 82.4% are representative of the overall situation in the EU, this would mean that each year, out of the 500 million passengers on whom PNR data are collected annually, approximately 50,000 passengers are subjected to "further examination" on the basis of a SIS II match, 40,000 of whom are relate to "Article 36 alerts", i.e., to "persons of interest" who are not (yet) formally wanted in relation to any crime (let alone a PNR-relevant one).**

But of course, there are also (confirmed) "hits" on other bases (including on the basis of "pre-determined criteria" and matches resulting from requests for information) – and other countries may also match against more than just Article 26 and Article 36 alerts on SIS II.

### (ab) Spontaneous provision of information to other PIUs on the basis of matches against lists and databases (including SIS II)

**It would appear that, until now, in practice, information – including information on matches against SIS II alerts – is only rarely spontaneously shared between PIUs.**

**However, the clear aim of the Commission is to significantly increase the number of spontaneous transmissions of PNR data and of information on (confirmed) "hits" against SIS II (or against pre-determined criteria: see below) between PIUs, and via PIUs to competent authorities in other EU Member States (again including intelligence agencies in Member States where those are designated as such).**

### (ac) Spontaneous provision of information to domestic competent authorities and to other PIUs on the basis of matches against pre-determined criteria

**It would appear that matching of PNR data against pre-determined criteria – and consequently also the spontaneous informing of competent authorities of (confirmed) "hits" against such criteria – is still extremely rare in the EU Member States. However, the aim is for the use of such criteria to be greatly expanded.**

### (ad) Spontaneous provision of "results of processing" of PNR data other than information on matches against list or databases (such as SIS II) or pre-determined criteria

**The spontaneous sharing of new or improved criteria is more likely to occur within the data mining *cadre* that is being formed (see above, at 4.9(fc)), rather than done through exchanges between PIUs. But that of course does not mean that it will not occur – on the contrary, the aim is clearly to extend the use of pre-determined criteria, and for the EU Member States to cooperate much more closely in the development and sharing of those criteria, specifically through a much-enhanced role for Europol.**

### (b) Provision of PNR data and analysis data to competent authorities, other PIUs or Europol on request

### (ba) Provision of information to domestic competent authorities at the request of such authorities

In relation to the provision of information by the PIUs to their domestic competent authorities at the latter's request, the relevant national rules apply. The Commission staff working document provides no information whatsoever on the extent to which this option is used beyond saying that the numbers are increasing.

In the Netherlands, some procedural safeguards are established to seek to ensure that requests are only made in appropriate cases, and in particular only in relation to PNR-relevant offences. Whether other Member States impose procedural safeguards such as prior authorisation of requests from certain senior officials, I do not know. The PNR Directive does not require them (it leaves this to the laws of the Member States) and the Commission staff working report does not mention them.

### (bb) Provision of information to competent authorities of other EU Member States at the request of such authorities

The Commission claims that provision of PNR data at the request of competent authorities of other EU Member States is one part of the PNR system that operates well. However, the Commission staff working report suggests that there are problems, in particular in relation to compliance with the purpose-limitation principle underpinning the PNR Directive: see below, at (d).

Moreover, if the Dutch data are anything to go by, **it would appear that the vast majority of requests for PNR data come from the national authorities of the PIU's own country**: in the Netherlands, in 2019-20, there were 3,130 requests from national authorities, against just 375 requests from other PIUs and authorities in other EU Member States.

This rather qualifies the Commission claim that "*the exchange of data between the Member States based on requests functions in an effective manner*" and that "*[t]he number of requests has grown consistently*". Both statements could be true, but **the actual total numbers of requests from other Member States may still be extremely low (for now), at least in comparison with the number of requests the PIUs receive from their own national authorities.**

### (bc) Provision of information to Europol at the latter's request

The Commission staff working document does not provide any information on the number of requests made by Europol, or on the responses to such requests from the PIUs.

The report on the evaluation of the Dutch PNR notes that within Europol there appear to be no procedural conditions or safeguards relating to the making of requests (such as the safeguard that requests from Dutch authorities must be checked by a Dutch prosecutor (OvJ).

**If the Dutch data are anything to go by, it would appear that there are in fact very view requests for information from Europol: in that country, the PIU only received 32 such requests between June 2019 and the end of 2020, i.e., less than two a month.**

**But if Europol is to be given a much more central role in the processing of PNR data, especially in the matching of those data against more sophisticated pre-determined criteria (with Europol playing the central role in the development of those more sophisticated criteria, as planned), the cooperation between the Member States' PIUs and Europol, and the sharing of PNR data and data on "hits", is certain to greatly expand.**

### (c) Transfer of PNR data to third countries on a case-by-case basis.

The transfer of PNR data by the Member States to countries outside the EU is only allowed on a case-by-case basis and only when necessary for fighting terrorism and serious crime, and PNR data may be shared only with public authorities that are competent for combating PNR-relevant offences. Moreover, the DPO of the relevant PIU must be informed of all such transfers.

However, the Commission reports that **four Member States have failed to fully transpose other conditions provided for by the Directive relating to the purposes for which the data can be transferred or the authorities competent to receive it, and two do not require the informing of the DPO.**

**It is seriously worrying that several Member States do not adhere to the conditions and safeguards relating to transfers of PNR data (and of "the results of processing" of PNR data – which can include the fact that there was a "hit" against lists or criteria) to third countries that may not have adequate data protection rules (or indeed other relevant rule of law-conform rules) in place. Some of the (unnamed) Member States that do not comply with the PNR Directive in this regard are likely to pass on such data in breach of the Directive (in particular, without ensuring that the data are only used in the fight against terrorism and serious crime) to close security and political allies such as the ones that make up the "Five Eyes" intelligence group: the USA, the UK, Australia, Canada and New Zealand.**

**This concern is especially aggravated in relation to the USA, which the Court of Justice has now held several times to not provide adequate protection to personal data transferred to it from the EU, specifically because of its excessive mass surveillance (and there are similar concerns in relation to the UK, in spite of the Commission having issued an adequacy decision in respect of that country).**

**Moreover, neither the Commission staff working document nor the Dutch report provides any information on how it is – or indeed can be – guaranteed that data provided in response to a request from a third country are really only used by that third country in relation to PNR-relevant offences, or how this is – or indeed can be – monitored.**

For instance, if data are provided to the US Federal Bureau of Investigation (FBI) in relation to an investigation into suspected terrorist activity, those data will also become available to the US National Security Agency (NSA), which may use them in relation to much broader "foreign intelligence purposes". That issue of course arises in relation to provision of information from any EU Member State to any third country that has excessive surveillance laws.

**Furthermore, if I am right to believe that the Dutch intelligence agencies have secret, unrecorded direct access to the PNR database (see above, at 4.10), they may also be sharing data from that database more directly with intelligence partners in other countries, including third countries, bypassing the whole PNR Directive system. Neither the Commission staff working document nor the report on the evaluation of the Dutch PNR law addresses this issue. And that issue, too, may well arise also in relation to other EU Member States.**

## (d) Subsequent use of the data and purpose-limitation

In principle, any information provided by the PIUs to any other entities, at home or abroad, or to Europol, is to be used by any recipient only for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, more specifically for the prevention, detection, investigation and prosecution of PNR-relevant offences. But it has become clear that this is far from assured in practice:

- because of the dilemma faced by PIUs in some EU Member States caused by the duty of any agency to pursue any offence that comes to their attention, the PIUs in some Member States pass on information also on (confirmed) "hits" relating to not-PNR-relevant offences (both spontaneously and in response to requests), and those data are then used in relation to the prevention, detection, investigation and prosecution of those not-PNR-relevant offences;
- in the Netherlands (and probably other Member States), once information is provided to a domestic competent authority, those data enter the databases of that authority (e.g., the general police databases) and will be subject to the legal regime that applies to the relevant database – which means that there is no guarantee that their subsequent use is in practice limited to PNR-relevant offences;
- when PNR data are provided by a PIU of one Member State to a PIU of another Member State (or to several or all of the other PIUs), they are provided subject to the purpose-limitation principle of the PNR Directive – but if those data are then provided by the recipient PIU(s) to competent authorities in their own countries, the same problems arise as noted in the previous indents;
- Member States take rather different views of what constitute PNR-relevant offences, and some make "broad and unspecified requests to many (or even all Passenger Information Units)" – suggesting that in this regard, too, the purpose-limitation principle is not always fully adhered to;
- within Europol there appears to be no procedural conditions or safeguards relating to the making of requests for PNR data from PIUs (such as the safeguard that requests from Dutch authorities must be checked by a Dutch prosecutor) and the Commission staff report does not indicate whether all the PIUs check whether Europol requests are strictly limited to PNR-relevant offences (or if they do, how strict and effective those checks are);
- "four Member States have failed to fully transpose … [the] conditions provided for by the Directive relating to the purposes for which [PNR data] can be transferred [to third countries] or [relating to] the authorities competent to receive [such data]";
- neither the Commission staff working document nor the Dutch report provides any information on how it is – or indeed can be – guaranteed that data provided in response to a request from a third country are really only used by that third country in relation to PNR-relevant offences, or how this is – or indeed can be – monitored;

  and

- if I am right to believe that the Dutch intelligence agencies have secret, unrecorded direct access to the PNR database, they may also be sharing data from that database more directly with intelligence partners in other countries, including third countries, bypassing the whole PNR Directive system. Neither the Commission staff working document nor the report on the evaluation of the Dutch PNR law addresses this issue. And that issue, too, may well arise also in relation to other EU Member States.

**In sum: There are major deficiencies in the system as concerns compliance, by the EU Member States, by Europol, and by third countries that may receive PNR data on a case-by-case-basis, with the fundamental purpose-limitation principle underpinning the PNR Directive, i.e., with the rule that any PNR data (or data resulting from the processing of PNR data) may only be used – not just by the PIUs, but also by any other entities that may receive those data – for the purposes of the prevention, detection, investigation and prosecution of PNR-relevant offences. *In simple terms: in this respect, the PNR system leaks like a sieve.***

### 4.12 The consequences of a "match"

It is quite clear from the available information that **confirmed "hits" and the associated PNR data on at the very least tens of thousands and most probably several hundred thousand innocent people are passed on to law enforcement (and in many cases, intelligence agencies) of EU Member States and to Europol – and in some cases to law enforcement and intelligence agencies of third countries – for "further examination"**. Many of those data – many of those individuals – will end up in miscellaneous national databases as data on "persons of interest", and/or in the Europol SIS II database as "Article 36 alerts". They may even end up in similar databases or lists of third countries.

**In terms of European human rights and data protection law, even the supposedly not-very-intrusive measures such as "only" being made the object of "discreet checks" constitute serious interferences with the fundamental rights of the individuals concerned – something that the European Commission and several Member States studiously avoided acknowledging at the Court hearing. More intrusive measure such as being detained and questioned or barred from flying of course constitute even more serious interferences. Both kinds require significant justification in terms of suitability, effectiveness and proportionality – with the onus of proof lying squarely on those who want to impose or justify those interferences, i.e., *in casu*, the European Commission and the Member States.**

Moreover, **in practice "watch lists" often become "black lists". History shows that people – innocent people – will suffer if there are lists of "suspicious", "perhaps not reliable", "not one of us" people lying around, and not just in dictatorships.**

That is yet another reason why those who argue in favour of such lists – and that includes "Article 36 alerts" and other lists of "persons of interest" "identified" on the basis of flimsy or complex criteria or profiles – bear a heavy onus to prove that those lists are absolutely necessary in a democratic society, and that the strongest possible measures are in place to prevent such further slippery uses of the lists.

# 5. The suitability, effectiveness and proportionality of the processing

## 5.1 The lack of data and of proof of effectiveness of the PNR Directive

Neither the European Commission's review nor the Dutch evaluation has come up with serious, measurable data showing that the PNR Directive and the PNR law are effective in the fight against terrorism or serious crime.

The Dutch researchers at least tried to find hard data, but found that in many crucial respects no records were kept that could provide such data. At most, some suggestions for better recording were made, and some ideas are under consideration, to obtain better data (although the researchers also noted that some law enforcement practitioners thought it would be too much effort).

To date, neither the Commission nor the Member States (including the Netherlands) have seriously tried to design suitable, scientifically valid methods and methodologies of data capture (*geeignete Formen der Datenerfassung*) in this context. Given that the onus is clearly on them to demonstrate – properly, scientifically demonstrate, in a peer-reviewable manner – that the serious interferences with privacy and data protection they insist on perpetrating are effective, this is a manifest dereliction of duty.

The excuse for not doing this essential work – that it would be too costly or demanding of law enforcement time and staff – is utterly unconvincing, given the many millions of euros that are being devoted to developing the "high risk" intrusive technologies themselves.

## 5.2 An attempt at an assessment

### (a) The appropriate tests to be applied

#### (aa) The general tests

In my opinion, the appropriate tests to be applied to mass surveillance measures such as are carried out under the PNR Directive (and were carried out under the Data Retention Directive, and are still carried out under the national data retention laws of the EU Member States that continue to apply in spite of the CJEU case-law) are:

**Have the entities that apply the mass surveillance measure – i.e., in the case of the PNR Directive (and the DRD), the European Commission and the EU Member States – produced reliable, verifiable evidence:**

**(iii) that those measures have actually, demonstrably contributed significantly to the stated purpose of the measures, i.e., in relation to the PNR Directive, to the fight against PNR-relevant crimes (and in relation the DRD, to the fight against "serious crime as defined by national law"); and**

**(iv) that those measures have demonstrably not seriously negatively affected the interests and fundamental rights of the persons to whom they were applied?**

If the mass surveillance measures do not demonstrably pass both these tests, they are fundamentally incompatible with European human rights and fundamental rights law.

This means the measures must be justified, by the entities that apply them, on the basis of hard, verifiable, peer-reviewable data.

### (ab) When a (confirmed) "hit can be said to constitute a "positive" result (and when not)

In the context of collecting and assessing data, it is important to clarify when a (confirmed) "hit can be said to constitute a "positive" result (and when not).

In my opinion, confirmed "hits" confirming the identity of "known" "persons of interest"/subjects of "Article 36 alerts" and the "identification" (labelling) of previously "unknown" persons by the PIUs as "persons who may be involved in terrorism or serious crime" can only be regarded as "positive" results under the PNR Directive if they result in those persons subsequently being formally declared to be formal suspects in relation to terrorist or other serious, PNR-relevant criminal offences.

### (b) The failure of the European Commission (and the Dutch government) to meet the appropriate test

The conclusion reached by the European Commission and Dutch Minister of Justice: that overall, the PNR Directive, respectively the Dutch PNR law, had been "effective" because the EU Member States said so (Commission) or because PNR data were quite widely used and the competent authorities said so (Dutch Minister) is fundamentally flawed, given that this conclusion was reached in the absence of any real supporting data.

*It is the equivalent to a snake oil salesman claiming that the effectiveness of his snake oil is proven by the fact that his franchise holders agree with him that the product is effective, or by the fact that many gullible people bought the stuff.*

*Or to use the example of Covid vaccines, invoked by the judge-rapporteur: it is equivalent to a claim that a vaccine is effective because interested parties say it is, or because many people had been vaccinated with the vaccine – without any data on how many people were protected from infection or, perhaps worse, how many people suffered serious side-effects.*

At the very least, the competent authorities in the EU Member States should have been required to collect, in a systematic and comparable way, reliable information on the outcomes of the passing on of (confirmed) "hits". Given that they have not done so – and that the Commission and the Member States have not even tried to establish reliable systems for this – there is no insight into how many of the (confirmed) "hits" actually, concretely contributed to the fight against PNR-relevant offences.

### (c) An attempt to apply the tests to the different types of matches

In my opinion, confirmed "hits" confirming the identity of "known" "persons of interest"/subjects of "Article 36 alerts" and the "identification" (labelling) of previously "unknown" persons by the PIUs as "persons who *may be* involved in terrorism or serious crime" can only be regarded as "positive" results under the PNR Directive if they result in those persons subsequently being formally declared to be formal suspects in relation to terrorist or other serious, PNR-relevant criminal offences.

*At the very least, the competent authorities in the EU Member States should have been required to collect, in a systematic and comparable way, reliable information on such outcomes. Given that they have not done so – and that the Commission and the Member*

*States have not even tried to establish reliable systems for this, there is no insight into how many of the (confirmed) "hits" actually, concretely contributed to the fight against PNR-relevant offences.*

However, the following can still usefully be observed as regards the lawfulness, suitability, effectiveness and proportionality of the different kinds of matches:

- Full PNR data are disproportionate to the purpose of basic identity checks;
- The necessity of the PNR checks against Interpol's Stolen and Lost Travel Document database is questionable;
- The matches against unspecified national databases and "repositories" are not based on foreseeable legal rules and are therefore not based on "law";
- The necessity and proportionality of matches against various simple, supposedly "suspicious" elements (tickets bought from a "suspicious" travel agent; "suspicious" travel route; etc.) is highly questionable; and
- The matches against more complex "pre-determined criteria" and profiles are inherently and irredeemably flawed and lead to tens and possibly hundreds of thousands of innocent travellers wrongly being labelled to be a person who "may be" involved in terrorism or serious crime, and are therefore unsuited (D: *ungeeignet*) for the purpose of fighting terrorism and serious crime.

### 5.3 Overall conclusions

The PNR Directive and the generalised, indiscriminate collection of personal data on an enormous population – all persons flying to or from, and the vast majority of people flying within, the EU – that it facilitates (and intends to facilitate) is part of a wider attempt by the European Union and the EU Member States to create means of mass surveillance that, in my opinion, fly in the face of the case-law of the Court of Justice of the EU.

In trying to justify the directive and the processing of personal data on hundreds of millions of individuals, the vast majority of whom are indisputably entirely innocent, the European Commission and the Member States not only do not produce relevant, measurable and peer-reviewable data, they do not even attempt to provide for the means to obtain such data. Rather, they apply "measures" of effectiveness that are not even deserving of that name: the wide use of the data and the "belief" of those using them that they are useful.

If proper tests are applied (as set out in sub-section 5.2(a), above), the disingenuousness of the "justifications" becomes clear: the claims of effectiveness of the PNR Directive (and the Dutch PNR Law) are based on sand; in fact, as the Dutch researchers rightly noted:

> **"There are no quantitative data on the way in which [and the extent to which] PNR data have contributed to the prevention, detection, investigation and prosecution of terrorist offences and serious crime."**

The Commission and the Member States also ignore the "high risks" that the tools used to "identify" individuals who "may be" terrorists or serious criminals entail. This applies in

particular to the use of algorithm/AI-based data mining and of profiles based on such data mining that they want to massively increase.

**If the Court of Justice were to uphold the PNR Directive, it would not only endorse the mass surveillance under the directive as currently practised – it would also give the green light to the massive extension of the application of (so far less used) sophisticated data mining and profiling technologies to the PNR data without regard for their mathematically inevitable serious negative consequences for tens and possible hundreds of thousands of individuals.**

**What is more, that would also pave the way to yet further use of such (dangerous) data mining and profiling technologies in relation to other large population sets (such as all users of electronic communications, or of bank cards). Given that the Commission has stubbornly refused to enforce the Digital Rights Ireland judgment against Member States that continue to mandate retention of communications data, and is in fact colluding with those Member States in actually seeking to re-introduce mandatory communications data retention EU wide in the e-Privacy Regulation that is currently in the legislative process, this is a clear and imminent danger.**

**The hope must be that the Court will stand up for the rights of individuals, enforce the Charter of Fundamental Rights, and declare the PNR Directive (like the Data Retention Directive) to be fundamentally in breach of the Charter.**

- o – O – o -

Douwe Korff (Prof.)
Cambridge (UK)
November 2021