COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 15 June 2015 T-PD(2015)11Résumé

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA
(T-PD)

Passenger Name Records, data mining & data protection:

the need for strong safeguards

=== E X E C U T I V E S U M M A R Y ===

Prepared by

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

with advice, comments and review by
Marie Georges
Council of Europe Expert

Directorate General Human Rights and Rule of Law

CONTENTS
of this Executive Summary

Introduction

Much has been said and written about Passenger Name Records (PNR) in the last decade and a half. When we were asked to write a short report for the Consultative Committee about PNR, "in the wider contexts", we therefore thought we could confine ourselves to a relatively straightforward overview of the literature and arguments.

However, the task turned out to be more complex than anticipated. In particular, the context has changed as a result of the Snowden revelations. Much of what was said and written about PNR before his exposés had looked at the issues narrowly, as only related to the "identification" of "known or [clearly 'identified'] suspected terrorists" (and perhaps other major international criminals). However, the most recent details of what US and European authorities are doing, or plan to do, with PNR data show that they are part of the global surveillance operations we now know about.

More specifically, it became clear to us that there is a (partly deliberate?) semantic confusion about this "identification"; that the whole surveillance schemes are not only to do with finding previously-identified individuals, but also (and perhaps even mainly) with "mining" the vast amounts of disparate data to create "profiles" that are used to single out from the vast data stores people "identified" as statistically more likely to be (or even to become?) a terrorist (or other serious criminal), or to be "involved" in some way in terrorism or major crime. That is a different kind of "identification" from the previous one, as we discuss in this report.

We show this relatively recent (although predicted) development with reference to the most recent developments in the USA, which we believe provide the model for what is being planned (or perhaps already begun to be implemented) also in Europe. In the USA, PNR data are now expressly permitted to be added to and combined with other data, to create the kinds of profiles just mentioned – and our analysis of Article 4 of the proposed EU PNR Directive shows that, on a close reading, exactly the same will be allowed in the EU if the proposal is adopted.

Snowden has revealed much. But it is clear that his knowledge about what the "intelligence" agencies of the USA and the UK (and their allies) are really up to was and is still limited. He clearly had an astonishing amount of access to the data collection side of their operations, especially in relation to Internet and e-communications data (much more than any sensible secret service should ever have allowed a relatively junior contractor, although we must all be grateful for that "error"). However, it would appear that he had and has very little knowledge of what was and is being done with the vast data collections he exposed.

Yet it is obvious (indeed, even from the information about PNR use that we describe) that these are used not only to "identify" known terrorists or people identified as suspects in the traditional sense, but that these data mountains are also being "mined" to label people as "suspected terrorist" on the basis of profiles and algorithms. We believe that that in fact is the more insiduous aspect of the operations.

This is why this report has become much longer than we had planned, and why it focusses on this wider issue rather than on the narrower concerns about PNR data expressed in most previous reports and studies.

The full report is structured as follows. After preliminary remarks about the main topic of the report, PNR data (and related data) (further specified in the Attachment), Part I discusses the wider contexts within which we have analysed the use of PNR data. We look at both the widest context: the change, over the last fifteen years or so, from reactive to "proactive" and "preventive" law enforcement, and the blurring of the lines between law enforcement and "national security" activities (and between the agencies involved), in particular in relation to terrorism (section I.i); and at the historical (immediately post-"9/11") and more recent developments relating to the use of PNR data in data mining/profiling operations the USA, in the "CAPPS" and (now) the "*Secure Flight*" programmes (section I.ii).

In section I.iii, we discuss the limitations and dangers inherent in such data mining and "profiling".

Only then do we turn to PNR and Europeby describing, in Part II. both the links between the EU and the US systems (section II.1), and then the question of "strategic surveillance" in Europe (II.ii).

In Part III, we discuss the law, i.e., the general ECHR standards (I); the ECHR standards applied to surveillance in practice (II, with a chart with an overview of the ECtHR considerations); other summaries of the law by the Venice Commission and the FRA (III); and further relevant case-law (IV).

In Part IV, we first apply the standards to EU-third country PNR agreements (IV.i), with reference to the by-passing of the existing agreements by the USA (IV.ii) and to the spreading of demands for PNR to other countries (IV.iii). We then look at the human rights and data protection-legal issues raised by the proposal for an EU PNR scheme. We conclude that part with a summary of the four core issues identified: purpose-specification and –limitation; the problem with remedies; "respect for human identity"; and the question of whether the processing we identify as our main concern – "dynamic"-algorithm-baseddata mining and profiling – actually works.

Part V contains a Summary of our findings; our Conclusions (with our overall conclusions set out in a box on p.); and tentative, draft Recommendations.

This Executive Summary reproduces the Introduction, the Preliminary remarks about PNR (etc.) and this last part (Part V) only.

Preliminary: what are PNR (and API and SFPD) data?

Passenger Name Records (PNRs) are records, created by airlines and travel agencies, relating to travel bookings. They are concerned with all the aspects of a booking – originally they were not primarily about the passenger or passengers: if a group booking was made, the personal details of the members of the group were often only added later (sometimes as late as the time of boarding). Wikipedia provides the following simple description:[1]

> In the airline and travel industries, a passenger name record (PNR) is a record in the database of a computer reservation system (CRS) that contains the itinerary for a passenger, or a group of passengers travelling together. The concept of a PNR was first introduced by airlines that needed to exchange reservation information in case passengers required flights of multiple airlines to reach their destination ("interlining"). For this purpose, IATA and ATA have defined standards for interline messaging of PNR and other data through the "ATA/IATA Reservations Interline Message Procedures - Passenger" (AIRIMP). There is no general industry standard for the layout and content of a PNR. In practice, each CRS or hosting system has its own proprietary standards, although common industry needs, including the need to map PNR data easily to AIRIMP messages, has resulted in many general similarities in data content and format between all of the major systems.
>
> When a passenger books an itinerary, the travel agent or travel website user will create a PNR in the computer reservation system it uses. This is typically one of the large Global Distribution Systems, such as Amadeus, Sabre, Worldspan or Galileo, but if the booking is made directly with an airline the PNR can also be in the database of the airline's CRS. This PNR is called the Master PNR for the passenger and the associated itinerary. The PNR is identified in the particular database by a record locator.
>
> When portions of the travel are not provided by the holder of the Master PNR, then copies of the PNR information are sent to the CRSes of the airlines that will be providing transportation. These CRSes will open copies of the original PNR in their own database to manage the portion of the itinerary for which they are responsible. Many airlines have their CRS hosted by one of the GDSes, which allows sharing of the PNR.
>
> The record locators of the copied PNRs are communicated back to the CRS that owns the Master PNR, so all records remain tied together. This allows exchanging updates of the PNR when the status of trip changes in any of the CRSes.
>
> Although PNRs were originally introduced for air travel, airlines systems can now also be used for bookings of hotels, car rental, airport transfers, and train trips.

For more formal purposes, there were (and still are) other records, in particular **Advanced Passenger Information (API**, held in the API System, **APIS**) and, in the United States of America, **Secure Flight Passenger data (SFPD)**. These latter records are essentially limited to travel document (passport) information and, in the case of API, basic information about the flights concerned.

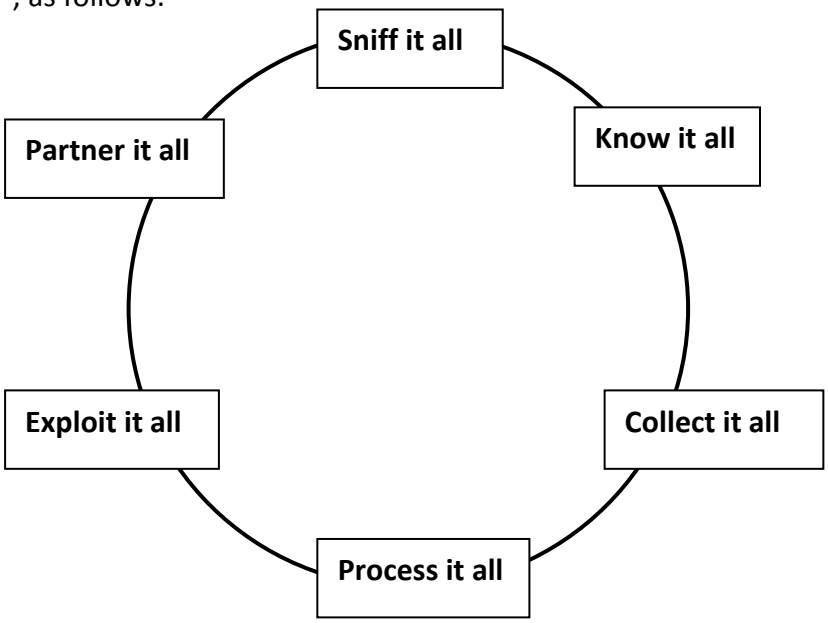
---

[1] See: https://en.wikipedia.org/wiki/Passenger_name_record

By contrast to API and SFPD, PNRs contain extensive information about the whole itinerary of the passenger(s) including hotel and car reservations (if booked with the flights), contact information including addresses, email- and IP-addresses and phone and mobile phone numbers, payment information (credit card details), dietary information (e.g., requests for vegetarian, kosher or hala'l meals), information on disabilities, etc., etc..[2]

For most of the 20th Century, state agencies were not generally interested in PNRs, except perhaps when they thought they might be relevant to ongoing criminal investigations, in which cases access to the records could be sought under the normal criminal procedures, typically with a judicial warrant.

This changed towards the end of the century, when the authorities in a range of countries started to become interested in using information technology more seriously in crime prevention and for more general "social engineering", and started to look at ways of using large collections of data to "identify" "targets" for policy action (see sub-section *III.i*, below). But the main impetus for the collection of large datasets for immigration-, law enforcement and national security purposes came from "9/11". In the USA, in particular, this led to a determination on the part of the authorities to adopt a massively broad approach to data collection, in particular in the fight against terrorism". This "**New Collection Posture**" is described in a slide used in a "top secret presentation [by the US's National Security Agency, NSA] to the 2011 annual conference of the Five Eyes alliance [of the intelligence services of the USA, the UK, Australia and Ne Zealand]", as follows:[3]



We discuss the links between this "new collection posture" – also epitomised in the name of the main early-21st Century US programme "**Total Information Awareness**" – and PNR data in sub-section *III.ii*, below.

[2] See the tables with the data fields required for SFPD, API and PNR in Attachment 1.

[3] The slide is reproduced in Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA and the Surveillance State, 2014, on p. 97.

Here, we should already note that we find later on, in our more detailed discussions of the demands for PNR, in relation to European human rights- and data protection law, that "traditional" passenger information such as API data (or SFPD data in the USA) suffice to meet all the requirements to "identify" "known" people who for some reason are "wanted" or otherwise "looked out for" by the authorities, be that for border control/immigration or normal law enforcement purposes (e.g., because they are wanted convicted criminals who are "on the run", or people formally held to meet the legal requirements of "suspect" under criminal procedure law, or who may be on some other "wanted" or "no-fly" list, perhaps because they are under a court order not to leave the country).

By contrast, we find that the only reason why the authorities – first in the USA, but now also in the EU, and in Russia, Mexico, the United Arab Emirates, South Korea, Brazil, Japan, Argentina and Saudi Arabia – would want full, "bulk" access to *all* the PNR records, on *all* travellers, is because they want to use the additional data for data mining and "profiling" purposes – or as they like to put it, in rather deceptive language,[4] so that they can "identify" "possible" or "probable" or even "potential" miscreants – especially "possible", "probable" or "potential" terrorists, but this is inevitably now being extended to even less-defined "extremists" (and in some of the countries just mentioned is likely to be extended to all manner of dissidents).

In other words, the demands for PNR data are part of the wider demands for suspicionless mass collection-, retention- and analyses of data: of e-communications data, financial transaction data, and now travellers' data and, especially, the linking and combining of those data.

More specifically, the data fields in PNRs with mobile phone information and credit card information obviously allow for easy linking of the PNR data to the other massive "bulk" data collections held by the intelligence agencies, on global e-communications and financial transactions.

The debates about the "proper" and "proportionate" use of PNR data, and about the possible risks and "disproportionate" uses to which they could be put, must therefore take place against these wider contexts: "PNR" is not an isolated issue, but a new symptom of a much wider disease.

This report tries to facilitate that wider debate.

[4] We discuss the sometimes deliberately confusing use of the words "identify", "identification" (and "misidentification") in section *IV*.

EXECUTIVE SUMMARY

Summary of findings

The facts

- The central problem with the demands for the provision of PNR in bulk to the authorities, is that this is – that this can only be – aimed at facilitating datamining and profiling by means of these records, linked to other major datasets (such as bulk communications data, or bulk financial transaction data) – as is clearly done in the USA and as is clearly also the main aim of the proposed EU PNR scheme: *full PNR data are simply not needed for any other, normal, legitimate law enforcement or border control purpose*.

- The demands for bulk data for such purposes are part of what used to be called by the USA "Total Information Awareness" – a programme that has not died but rather, has been re-surrected in the USA's new "New Collection Posture" under which the USA effectively seeks access to all information available through the Internet and global IT networks, as exposed by Edward Snowden.

- No serious, verifiable evidence has been produced by the proponents of compulsory suspicionless [bulk] data collection to show that datamining and profiling by means of the bulk data in general, or the compulsory addition of bulk PNR data to the data mountains already created in particular, is even *suitable* to the ends supposedly being pursued – let alone that it is *effective*. Yet in law (as noted under the next heading), the onus to proof o such suitability and effectiveness rests on those who demand the introduction or continuation of such measures.

- Such datamining and profiling is used in the USA, and is clearly intended to be used in the EU, at rating people on a risk scale (e.g., as "high risk") on anti-terrorist lists, on the basis of such datamining and profiling (see in particular the discussion of the "Fourth List" noted by the US GAO, in Part I, section I.ii, of the report).

  [NB: As noted below, the proposed EU PNR scheme is aimed at facilitating the creation of similar "dynamic"-algorithm-based lists.]

- However, such lists are by their very nature of highly dubious reliability, with inevitably many "false positives", i.e., people being wrongly labelled as "high risk" on an anti-terrorist database (cf. the discussion of the "*baserate fallacy*" in Part I, section I.iii of the report).

- Yet these lists are widely shared by the USA, with reportedly at least 22 other countries – without any of the recipient countries being in any way able to understand, let alone challenge, the "high-risk" designation of individual passengers.

- There have already been cases of people being wrongly labelled on such lists and, consequently, handed over to repressive regimes and tortured (see, e.g., the Maher Arar case discussed in the final section of the report).

- There is also a high risk of such datamining and profiling resulting in "discrimination by computer" (as discussed under that heading in Part I, section I.iii of the report). Crucially, given the misplaced focus on the use of "sensitive data" in profiling, such discrimination can result from profiling that does not use any such data, or even any proxies for such data (such as meal preferences). Rather, algorithms can reinforce much more deeply and insiduously embedded social distinctions, linked to almost any kind of matter (e.g., postcode or length of residency). This has implication in terms of human rights- and data protection law, as noted under the next heading.
- Yet at the same time, by the very nature of a list created by algorithms applied to inherently ambiguous and subjective "intelligence", such determinations, and such discriminatory outcomes, are extremely difficult to challenge – and they become effectively unchallengeable if the underlying "intelligence" and the evaluations of the "intelligence" and the precise algorithm used to weigh the various elements of the "intelligence" cannot be challenged. As of course no victim of such a determination will ever be able to do.
- Proposals to provide some form of "algorithmic accountability" (Citron), or to use "reverse engineering" to counter such dangers (Diakopolous) are in practice impossible to use in relation to secretive law enforcement/border control/national security databases. As noted under the next heading, this means that there are, in reality, no effective remedies against such wrong labels or discriminatory outcomes of the profiling by the relevant agencies.
- The latest (2012) EU-US PNR Agreement does not stand in the way of the PNR data transferred to the USA under the agreement being fed into these kinds of wider anti-terrorist databases, in order to "identify" "high-risk" passengers: the use of the data for such "identification" is clearly allowed, but the word "identification" is here used, misleadingly, not to match PNR data on lists of "known" terrorists or other serious criminals, but to rate the passengers on a risk scale, on the basis of dynamic-algorithm-based profiling.
- Edward Hasbrouck has shown that in any case, the USA are completely by-passing the EU-US PNR Agreement, in that they can already obtain full access to the vast bulk of PNR data – including full PNRs on most intra-European flights – from the Computerised Reservation Systems of the airlines and travel agencies, that are housed (or mirrored) in the USA.
- The proposed EU PNR Directive, read closely, is clearly aimed at facilitating the creation of similar "dynamic"-algorithm-mined databases, resulting in similar "identifications" of people as "high risk" (or as "posing serious danger", to use another euphemism that crops up in the literature), i.e., as similarly labelling them in this way on the basis of inherently fallible analyses (see Part II, section II.ii).
- Unsupringly, many other countries are now also beginning to demand the handing over of PNR data in bulk. So far, this includes Russia, Mexico, the United Arab Emirates, South Korea, Brazil, Japan, Argentina and Saudi Arabia.

- The EU intends to provide for "horizontal" rules on the provision of PNR data, by European airlines, to these (and any other) countries. However, how could these regulate the labelling of people by such countries according to their own definitions of "high risk"? If Western countries already want to extend close surveillance and other repressive measures to "extremists-who-have-not-yet-broken-the-law" (as David Cameron is explicitly suggesting), how will these "horizontal" rules prevent the targeting of non-criminal dissidents by those other countries, on the basis of similar algorithm-based profiling? And if Western countries already themselves fail to counter the danger of algorithms creating "suspect communities" and leading to "discrimination-by-computer", how will these rules address those wrongs in those other states?
- There have as yet been no Russian or Chinese "Edward Snowdens", but it would be surprising if China and Russia, at least, would not already be building – or already have in operation – such "rule-based" surveillance and analysis systems. Will the "horizontal" EU rules allow the feeding of PNR data from EU airlines into those systems? How would they prevent that?

The law

- The general requirements of the European Convention on Human Rights in relation to targeted surveillance, as developed by the European Court of Human Rights, are summarised in a text box in the report, on p. 46.
- These general principles are important, e.g., by clarifying that even targeted but secret use of PNR data would have to be restricted to particularly serious crimes, and to strictly limited categories of people (with at least some link to serious criminal or terrorist activity); and that any such uses should be subject to strict substantive and procedural safeguards and "effective remedies".
- Moreover, any "general surveillance" based on bulk PNR data should be based on statute law; and all the main rules on how it is to be carried out should be clear and made public, so that they can be "foreseeable" in their application.
- We conclude from this that, for instance, the meaning of the word "identification" should be made clear in the rules (and any accompanying documentation, such as Explanatory Memoranda to draft laws), in particular when the term is used, not to indicate finding a "known" person (typically, a person on a list), but to indicate a "risk" rating, a labelling, rather than such direct "identification".
- Also, as the Venice Commission has said, one "implication of the ECtHR's approach is that there must be [published] legal authority for issuing selectors as regards the content of the data, and as regards metadata, for issuing instructions for contact-chaining and otherwise analyzing this data." Of course, the exact terms used as "selectors" need not be published, but the basic structure of the analyses should be transparent.
- However, the implication drawn by the Venice Commission can relate only to fairly straight-forward use of pre-specific "selectors". It is in practice impossible to pre-specify any algorithm that might be used to "dynamically" "improve" the datamining/profiling, e.g., by creating further (combinations of) selectors by

means of "artificial intelligence" and the adding of different (and also dynamically changed) "weight" to the different selectors.

- In this respect, it is important to note that it follows from the European Court of Human Rights judgment in the case of *Segerstedt-Wiberg and Others v. Sweden*, discussed in Part III, section III.i, at IV, that people should not be subjected to "filtering" or datamining based on tenuous links with organisations which do not pose any real, active threats to national security. This has obvious implications in relation to allegedly "extreme" – but not actively violent – Islamist groups too.
- Any "selectors" that put under surveillance organisations, or anyone with links to organisations, that may appear to be "extremist" but that have not actually engaged in violence or terrorism would in our opinion be in contravention of this judgment.
- It is an essential requirement of the ECHR and the EU Charter, and indeed of the rule of law, that there must be "effective remedies" against violations of individual rights. In the *Segerstedt-Wilburg* case, the Court reaffirmed what it had already held in *Klass* and other earlier cases: that in relation to secret surveillance this "need not necessarily in all cases" require a judicial remedy (although that is clearly the best option) – but it expanded on the relevant requirements to stress that any effective remedial body must have full powers to fully investigate a complaint about secret files or secret surveillance; and full powers to order the destruction or correction of the file, and/or its release to the individual concerned – and the State must provide evidence that those powers are also actually and effectively exercised in practice.
- In our opinion, a somewhat obscure remark in the judgment relating to the sufficiency of internal supervisory mechanisms while secret surveillance is carried out is clearly limited to brief, targeted telephone interception, and does not apply to long-term analyses of bulk data: the obtaining and further processing, including any datamining/profiling of such data must always be subject to the full powers of fully independent bodies, just mentioned.

ALL OF THE ABOVE IS IMPORTANT. HOWEVER, WE HAVE FOUND THAT THE KIND OF "DYNAMIC"-ALGORITHM-BASED DATAMINING AND PROFILING WE HAVE FOCUSED ON RAISES EVEN MORE FUNDAMENTAL ISSUES IN TERMS OF THE EUROPEAN CONVENTION OF HUMAN RIGHTS AND THE EU CHARTER, AND THUS ALSO IN TERMS OF THE COUNCIL OF EUROPE DATA PROTECTION CONVENTION. SPECIFICALLY:

- Such special, dangerous processing must be assesed especially strictly in regards to the question of whether it serves – can ever be said to serve – a "legitimate aim" in a democratic society; or in data protection terms: whether there is a clear and acceptable "specified" purpose and whether the processing is indeed limited to that purpose – *if it does not, that means that it is* ipso facto *in violation of the ECHR and the EU Charter, and of the Data Protection Convention*;
- The effectiveness of any supposed remedies against such processing must also be especially strictly scrutinsed – *if there are no actually effective remedies in place, or available, that too would in itself violate those instruments*;

- Most especially, such processing of personal data should never touch on the "essence", on the "untouchable core" of the rights in question, i.e., of the right to private life and the right to data protection – *if it did, it would again be incompatible with these instruments at the most fundamental level*;

  And at a more prosaic (but still crucial) level:

- Such special processing must at the very least be capable of achieving the purported purpose for which it be used; it must be "suited to" that aim – *if it is not, the processing can never be regarded as "necessary" or "proportionate" to that aim, and would therefore also on that basis be in violation of these instruments*

We have concluded that in all four of these fundamental respects, "dynamic"-algorithm-based profiling, aimed at rating individuals on a "risk scale" (e.g., "high risk") on an anti-terrorist database, fails to meet these requirements, as further explained in our Conclusions, below.

Conclusions

As noted above, we have drawn important conclusions on the use of bulk PNR data in respect of four fundamental issues:

The compulsory suspicionless provision of PNR data in bulk does not serve a legitimate aim:

As already noted, we found that bulk PNR data are not needed for any normal, legitimate law enforcement or border control purpose (API suffices for those). Rather, we concluded that the only real purposes of the demand for bulk PNR data is to serve either of the two following purposes:

- pro-active "identification" of "possible suspects", i.e., the marking of people as a "probable criminal" or "possible criminal", without those people being yet formally categorised as suspects in the criminal law/criminal procedure law sense (i.e., in the absence of any evidence against them that would suffice to properly designate them as formal suspects, in accordance with criminal procedure law); and
- pro-active "identification" of people for "preventive targeting" on national security grounds, in cases in which no action can (yet) be taken against them under the criminal law –
- on the basis of "dynamic"-algorithm-based datamining and profiling.

In other words, the demands for PNR data are part of an attempt at "predictive policing" or "predictive protection of national security": the *Vorverlegen* or "bringing forward" of state intrusion, to "deal" with people who are not (yet) breaking the law, but who are either labelled as "probably" or "possibly" being a terrorist or other criminal, or "predicted" to "probably" (or even "possibly") become one in future.

In our opinion, it cannot be acceptable in a society under the rule of law that intrusive measures are used to "target" people who have done no wrong – not even on the basis that "the computer says" that they are at some dubiously-calculated "risk" of doing some wrong in the future, or similarly dubiously calculated to have "possibly" or indeed

"probably" been involved in any wrong, without the kind of evidence (even preliminary evidence) that states under the rule of law require for the imposition of repressive measures.

As the case of Maher Arar shows, being thus labelled on a list is not without consequences – indeed possible extreme consequences.

In other words: "dynamic"-algorithm-based datamining and profiling with the aim of such "predictive" or "preventive" labelling of people on a "risk scale" is not a "legitimate aim" in a democratic society, and is therefore inherently fundamentally incompatible with the European Convention of Human Rights and the EU Charter of Fundamental Rights.

This ought to suffice to reject any plans to allow PNR data, or any bulk data on general populations, for large-scale datamining and profiling.

However, we will still also consider the other three fundamental objections mentioned.

There are no effective remedies against the outcomes of "dynamic"-algorithm-based datamining and profiling:

We have concluded that there simply are no currently available, let alone operational, remedies against the dangers of people being mis-labelled as "high risk" on an anti-terrorist list as a result of deficiencies in the algorithms used, or against discrimination-by-computer caused by the algorithms.

Crucially, you simply cannot remedy such wrongs by "improving" the algorithm, or by adding more data: the dangers are inherent in the processes and can only be countered, if at all, by deep analyses and auditing of the results of the datamining.

There is no indication whatsoever that such deep analyses and audits are actually carried out with the aim of protecting innocent people from being wrongly labelled.

Until such analysis- and audit systems are in place, and are made transparent – with involvement of critical scientists and human rights and data protection advocates – "dynamic" algorithm-based profiling should not be permitted in a state under the rule of law.

In simple human rights and data protection terms: there are no effective remedies available against anti-terrorist/national security "dynamic" algorithm-based datamining and profiling – and without such remedies such operations are simply not compatible with the European Convention on Human Rights, the EU Charter of Fundamental Rights, or the Council of Europe Data Protection Convention.

Or to put it at its absolute mildest:

The conclusion must be that either "dynamically-improved" algorithms should be regarded as intrinsically contrary to the ECHR, because they cannot be properly controlled; or that actually effective means of controlling them must be found, e.g., to check on how reliable the application of the algorithms is: how many "false positives" and how many "false negatives" did they generate? And were the results (unintentionally) discriminatory?

As noted in the report that is a much bigger challenge than is acknowledged by the proponents of those systems.

"Dynamic"-algorithm-based datamining and profiling, in particular if aimed at rating people on a "risk scale" on an anti-terrorist list, violates the most fundamental duty of the State and the EU to "respect human identity":

We believe that "preventive" or "predictive" profiling of individuals on the basis of essentially unverifiable and unchallengeable "dynamic"-algorithm-based bulk data, unrelated to any specific indications of wrongdoing, and without any targeting on the basis of such suspicions touches on the "essence", the untouchable core of the right to privacy – and indeed violates the even more fundamental principle underpinning the right to privacy (and other rights), that states must respect "human identity".

In our opinion, the PNR instruments allowing for such datamining and profiling are thus, on this basis too, incompatible with European legal principles of the most fundamental kind.

Trying to "identify" "possible" or "probable" terrorists by means of "dynamic"-algorithm-based datamining and profiling does not work:

Profiling and mining large datasets with the aim of "identifying" rare phenomena, such as the small number of terrorists in the general population (or even in more specific populations) inevitably suffers from the "*baserate fallacy*", leading to unacceptably high number of "false positives" (people wrongly labelled a "possible" or "probable" terrorist, or generally as "high risk"), or "false negatives" (actually terrorists not being identified), or both.

It has been acknowledged by the US National Research Council and others that the US datamining operations have not stopped any terrorist attack.

The EU Member States and the European Commission have failed to provide any serious, scientifically verifiable data in support of their claims that bulk PNR data does work in identifying terrorists, or indeed that other bulk datasets, specifically compulsorily retained communications data, have had any impact on law enforcement clear-up rates.

The largest and most serious study into possible efficacy of bulk data retention, by the Max Planck Institute at the request of the European Commission, discussed in Part xxx of the report, found that:

> there are no indications that compulsory suspicionless [e-communications] data retention has in the last years led to the prevention of any terrorist attack.

There is still no serious effort on the part of those who clamour, not just for continuing communications data retention, but also for further bulk "just-in-case" collections, such as the compulsory provision of full PNR data, to actually provide any serious, meaningful, scientifically valid evidence to show the efficacy of the measures in fighting serious crime or terrorism.

Yet under the ECHR and the EU Charter, the onus is on them to show convincing evidence of the effectiveness of bulk data collection and –analyses. This duty is the more onerous in view of the very serious interferences with human rights inherent in such collection and analyses (as noted above).

The fact that they have not provided any such evidence, in our opinion, simply underlines the scientific doubts about the efficacy of datamining in these regards: the proponents of bulk data collection, -mining and –profiling do not provide any real evidence of the efficacy of their "dynamic"-algorithm-based system, because they simply DO NOT WORK.

This ought to suffice in simple practical terms to abandon these highly-intrusive and dangerous efforts. But in more legal terms, it means "dynamic"-algorithm-based datamining and profiling are simply not "appropriate", not "suited" to the proclaimed aim of "identifying" terrorists from large datasets – and thus also not "necessary" or "proportionate" in relation to any legitimate law enforcement or anti-terrorist actions.

In other words, our overall conclusions are that:

- **The compulsory suspicionless provision of PNR data in bulk does not serve a legitimate aim;**
- **There are no effective remedies against the outcomes of "dynamic"-algorithm-based datamining and profiling;**
- **"Dynamic"-algorithm-based datamining and profiling, in particular if aimed at rating people on a "risk scale" on an anti-terrorist list, violates the most fundamental duty of the State and the EU to "respect human identity";**

and on top of that:

- **Trying to "identify" "possible" or "probable" terrorists by means of "dynamic"-algorithm-based datamining and profiling does not work.**

Recommendations

NB: We have been asked by the Consultative Committee to draft recommendations that the Committee itself might wish to adopt. We provide a number of those below. However, it is of course entirely up to the Committee to decide whether to make any of these draft, tentative recommendations its own.

The Consultative Committee recalls that European human rights- and data protection law requires, *inter alia*, that:

- All requirements that personal data should be provided to law enforcement-, border control- or national security agencies "in bulk" should be clearly set out in clear and precise statute law; and all subsidiary rules that are necessary to enable individuals to foresee the application of the statutory rules, should be equally clear, and made public. Only the lowest, operational guidance-type rules might be kept secret, and even then only as long as they do not contradict of obscure the application of the published rules. This also applies to any requirements that PNR data be handed over to state (or international) authorities in bulk;
- The application of all those rules in practice should be subject to serious, meaningful transparency and accountability;[5] and that
- There should be full and effective remedies against the use of bulk data, including bulk PNR data, in "general surveillance".

In that regard, the Consultative Committee notes that the Secretary-General of the Council of Europe has been urged, *inter alia*, by the Parliamentary Assembly of the Council of Europe, to use his power under Article 52 of the European Convention to demand that all CofE Member States provide full account of any "general surveillance" of the kind exposed by Edward Snowden that they may be involved in, with clarification on how this accords with their obligations under the ECHR.

The Consultative Committee supports this call, and recommends that when the Secretary-General does issue such a demand, he specifically also asks the Member States:

- whether they use any bulk data they acquire for any datamining and profiling in order to "identify" "possible" (or "probable") terrorists – with full clarifications of what exactly this "identification" entails (i.e., whether it merely involves matching PNR data against lists of "known" people, or whether it involves rating people on "risk scales" that are reflected in anti-terrorist databases);
- what safeguards are in place against straightforward mis-identifications on such lists,

but also especially:

[5] We have not addressed this issue in the report, because it would have exceeded our brief. We note however the very useful *Issue Paper* of the Council of Europe Commissioner for Human Rights on Democratic and effective oversight of national security services (May 2015), and the Venice Commission "Update of the 2007 Report on The Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies (April 2015), which provide important indicators in this area, of which the Consultative Committee should take account.

- how they guard against erroneous risk ratings of such kind; and why they believe any such redress and remedial action is effective.

Pending the provision of information that might lead to another conclusion, the Consultative Committee believes that the use of "dynamic"-algorithm-based datamining and profiling with the aim of "predictive" or "preventive" labelling of people on a "risk scale" is *not a "legitimate aim" in a democratic society*, *touches on the "essence", the untouchable core, of the right to private life and the right to data protection*, and would appear to be *unsuited to* the aim of actually identifying real terrorists – and thus *neither necessary nor proportionate* to that aim; and is therefore *fundamentally incompatible* with the European Convention of Human Rights, the EU Charter of Fundamental Rights – and with the Council of Europe Data Protection Convention of which the Committee is a guardian;

And therefore recommends:

- That "dynamic"-algorithm-based datamining and profiling for the purpose of "identifying" "possible" (or "probable") terrorists on the basis of a computer assessment by any State party to the Data Protection Convention be stopped immediately; and
- That the passing on of PNR data to any non-State Party for the purpose of such "dynamic"-algorithm-based profiling, or that may result in the use of the data in such processing by the non-State Party be also stopped; and
- That serious scientific studies are commissioned as a matter of urgency of appropriate independent scientist, with the involvement of human rights- and data protection advocates and civil society, to evaluate the effectiveness or ineffectiveness of such processes for such purposes, in particular also in terms of "false positives" and "false negatives", and in relation to the question of whether such datamining and profiling can or did lead to discriminatory outcomes; and to examine if effective, scientifically sound, means can be developed to counter such negative outcomes (or whether this is impossible).

- o – O – o -

DK/MG, June 2015