Passenger Name Record Agreements: The Umpteenth Attempt to Anticipate Risk

Francesca Galli

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Article

AUTHOR

Francesca Galli

CITATION SUGGESTION

F. Galli, "Passenger Name Record Agreements: The Umpteenth Attempt to Anticipate Risk", 2010, Vol. 5(3), eucrim, pp124–131. DOI: https://doi.org/10.30709/eucrim-2010-03

Published in
2010, Vol. 5(3) eucrim pp 124 – 131
ISSN: 1862-6947
https://eucrim.eu

Over the last decade, the United States and the European Union have become increasingly important partners in combating terrorism and have further developed intertwined security interests.

The signing of the so-called SWIFT II agreement[1] on 28 June 2010 (approved by the European Parliament on 8 July 2010) raises, once again, issues concerning the potential conflict between data protection and security matters in the context of transatlantic cooperation.[2] The aim of this instrument is

"to make sure that designated providers of international financial payment messaging services (and primarily the company "Swift") make available to the United States Department of the Treasury financial payment messaging data stored in the territory of the European Union necessary for preventing and combating terrorism and its financing."

In fact, a great amount of the data managed by Swift will soon be stored only in the EU and no longer in the US.

The debate surrounding the adoption of the new instrument gives civil libertarians another chance to discuss the evolving content of the controversial PNR agreements. Indeed, although the PNR agreement signed by the Council in July 2007[3] would only expire in 2014, the entry into force of the Lisbon Treaty requires the consent of the European Parliament in order for the agreement to be formally concluded and to preserve its legal effect.

Legal and Factual Background

The use of databases and the cross-referencing of elements to identify suspects has long been a powerful tool for law enforcement authorities in the prevention and prosecution of organized crime. In the aftermath of September 11, information exchange and information sharing was seen as crucial in the fight against terrorism.

Within this framework, US law enforcement authorities asserted the need to monitor and control flights over their territory. In fact, as many as 400 flights depart for the US each day from around 80 different European destinations. The US Aviation and Transport Security Act of 19 November 2001 (as amended by the 2004 Intelligence Reform and Terrorism prevention Act), required airlines that operate passengers to, from, or through the US to provide advance information on air travelers by means of the US customs and border patrol access to the electronic Passenger Name Records.[4]

Airlines were thus confronted with a dilemma: either facing severe fines and possibly the loss of landing rights if they refused to forward the information requested or infringing the data protection rules enshrined in the EU Data Protection Directive in order to respond to the security request made by the US.

The Data Protection Directive entered into force in 1995 to regulate the transfer of personal data within the EU and to third countries. It provides several fundamental principles that are at the heart of the current right to data protection as recognized in the EU: the principle of fair and lawful processing of data; the purpose limitation principle (the gathering of personal data requires specified, explicit, and legitimate purposes – the collection of data for future purposes and their use for purposes other than those for which they were collected or compatible therewith is prohibited); the principle of transparency; and the right of individuals to access and to redress personal information. Most importantly, according to Art. 25(1), the transfer of personal data from EU Member States to third countries may take place only where the third country in question ensures an adequate level of data protection.

At the source of the dispute is the fact that the concept of privacy and of data protection is approached in a completely different manner in the EU (where Member States' views are far from being harmonized) and in the US. In US constitutional law, the right to privacy is conceived as a restriction of the powers of the government to interfere with citizens' private lives. The right to privacy does not convey the idea that citizens should be able to monitor and control how their personal data are derived, analyzed, and processed. Individual privacy and personal data are not protected directly but through a combination of provisions, each of a different nature (constitutional law, Supreme Court case-law, sector-specific legislation, etc.) leading to a piecemeal result.[5]

The EU Commission had to find an agreement in order to reconcile two opposite necessities and strike a provisional balance between the different issues at stake: not only the prevention of crime and terrorism as well as the protection of fundamental rights but also the fragile EU/US relationship.

In an Area of Freedom, Security and Justice, allegedly becoming all the more an area of only security, PNR agreements have not always been considered a necessary and proportionate measure to fight terrorism.[6] At times, the European Parliament expressed doubts as to the adequate level of data protection in the US and fiercely criticized successive PNR agreements, not always considered a necessary and proportionate measure to fight terrorism. The European Data Protection Supervisor and Art. 29 Working Party raised similar concerns as to the impact on fundamental rights and the need to redraft the agreements to introduce better safeguards.[7]

Parliaments' actions led to the pronouncement of the judgment of the European Court of Justice on 30 May 2006 aimed at the 2004 PNR agreement.[8] The Court addressed the Commission adequacy decision, recognizing that, as required by Art. 25(1) of the Data Protection Directive, the US provide an adequate level of protection for the transfer of PNR information; the international agreement was concluded on the basis of such decision by the Council. The Luxembourg Court held that the agreement had been concluded on the wrong legal basis (art 95 TUE) as it pertains to third pillar security issues and not first pillar commercial matters.

However, to the disappointment of civil libertarians, the ECJ annulled the PNR agreement without touching upon its content or assessing whether fundamental rights had been infringed. The ECJ judgment focused on a rather technical issue and did not amount to a key decision on the balance between liberty (and particularly the right to privacy) and security in the aftermath of September 11. There were no major changes in the newly negotiated agreement.

Causes for Concern

Firstly, the *purpose of the agreement* is too broad and vague. It is not limited to counter-terrorism purposes but is directed at "other serious crime including organized crimes that are transnational in nature." The vagueness of this wording allows great discretion in its interpretation and the consequent application of the agreement. Thus, it raises not only legal certainty issues but also concerns in relation to the balance between the necessity of this measure and the intrusiveness of state intervention in this context.

Secondly, the *quality and proportionality of the data* is problematic: PNR are a particularly expansive category, which can include sensitive information such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, and/or data concerning health or sex of the individual. The gathering of sensitive data without any judicial oversight, coupled with the lack of accountability and a broad definition of the scope of the PNR agreement, could give a renewed impetus to racial profiling. This selective practice implies the reliance upon group characteristics such as race, national or

ethnic origin, and religion as part of a profile to determine the targets of preventive police power. In the absence of any objective criteria to identify those individuals who belong to the category of "dangerous people," sensitive data could establish policing on prejudice about identity and racial profiling so that criteria such as race, religion, and ethnicity are considered and used as indicators of dangerousness under counter-terrorism policies.

In addition, PNR agreements allow for a bulk collection of personal data as it is not focused on individuals supposedly presenting a risk. Risk assessment analyses are thus carried out in an undifferentiated manner, from terrorist suspects and alleged criminals to innocent passengers. Such wide scale data gathering, analysis, and storage raises legitimacy and proportionality issues and is potentially in conflict with the right to privacy under Art. 8 ECHR as interpreted by the Strasbourg Court. In *S and Marper v UK* (2008), the ECtHR noted that the British legislation on the retention of DNA samples failed to strike a proper balance between public and private interests, the power of retention having a "blanket and indiscriminate nature." The Court highlighted that

"it is as essential to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."[9]

The access to PNR data is not simply meant for identification purposes but is supposedly useful to deduce the dangerous or suspicious intention of passengers who are worth further investigation. Data mining programmes are able to generate automated profiling based on PNR information and computer-generated risk assessment scores to identify passengers who may pose a risk without being on any government's watch list. A wrongful interpretation of the information provided by the computer could, however, lead to misleading conclusions.

While personal data must be collected and analyzed accurately, the quality of the assessment could be biased by the fact that PNR information are collected by airlines for commercial purposes, with low data protection standards, and then used for public security purposes by law enforcements authorities.

Civil libertarians have also repeatedly questioned the duration of the storage itself and the possibility to share personal data with agencies that are not responsible for counter-terrorism and thus would use it for different purposes. A comparison with similar PNR agreements concluded with Australia and Canada shows that a more complex regulatory framework of safeguards is attainable.[10]

Liberty vs. Security

These issues have to be placed in the greater context of the balance between liberty and security and the numerous competing interests existing in this area. How is the protection of personal data balanced against the need for security? Is the gathering and sharing of personal information the price to be paid for enhanced security or simply abuse of the right to privacy?[11]

There has been a lot of misleading public debate about the alleged opposition between data protection law and security concerns of governments and law enforcement agencies. In fact, a possible hindrance to the investigation and prosecution of criminal offences and criminals constituted by data protection provisions is simply a myth. Nonetheless, a number of questions arise as to the boundaries of both data protection provisions and security measures. In particular, the access of law enforcement authorities to personal data of individuals who are not suspected or convicted of a criminal offence should be strictly limited and

regulated. The fight against organized crime should not allow the indiscriminate use of data collected for one purpose (e.g., commercial purposes) for a different one.

The Prediction and Prevention of Future Risks

In the context of PNR agreements, there is an increasing quantity of data to be processed and analyzed. Such an analysis has the ambitious purpose not only of spotting known or potential terrorists but also of carrying out risk assessments of individuals prior to boarding. PNR agreements apply to all passengers regardless of whether they are suspected of having committed or being about to commit an offence. However, they do not specify how and on the basis of which criteria personal data are processed to carry out such risk assessment.

In a broader context, the growing threat represented by terrorism and organized crime has modified the means and legitimization of state intervention placing risks and damage control at its centre. For instance, the criminologists Feeley and Simon describe a risk management strategy for the administration of criminal justice aiming at securing at the lowest possible cost-dangerous classes of individuals.[12] The focus is on targeting and classifying suspect groups and making assessments of their likelihood to offend in particular circumstances or when exposed to certain opportunities.

There is a need to act with great urgency to cope with potential risk, and there is no time to obtain a clear view on whether there would be sufficient evidence to support an investigation or a prosecution. Law enforcement authorities hence act on the lower standard of risk rather than on proof of criminal activities for purposes connected with protecting members of the public from a risk of terrorism.

Policy-making and crime-fighting strategies are increasingly concerned with the prediction and prevention of future risks (in order, at least, to minimise their consequences) rather than the prosecution of past offences.[13] Zedner describes a shift towards a society "in which the possibility of forestalling risks competes with and even takes precedence over responding to wrongs done,"[14] and where "the post-crime orientation of criminal justice is increasingly overshadowed by the pre-crime logic of security."[15] The crime prevention logic is characterised by "calculation, risk and uncertainty, surveillance, precaution, prudentialism, moral hazard, prevention and, arching over all of these, there is the pursuit of security." An analogy has been drawn with the "precautionary principle" developed in environmental law in relation to the duties of public authorities in a context of scientific uncertainty, which cannot be accepted as an excuse for inaction where there is a threat of serious harm.[16]

Although it certainly existed prior to September 11, the counter-terrorism legislation enacted since then has certainly expanded all previous trends towards anticipating risks. The aim of current counter-terrorism measures is mostly that of preventive identification, isolation, and control of individuals and groups who are deemed dangerous and allegedly represent a threat to society. The risk in terms of mass casualties resulting from a terrorist attack is thought to be so high that traditional due process safeguards are considered unreasonable or unaffordable, and prevention becomes a political imperative. In the words of the UK Anti-Terrorism Branch:

"The threat from international terrorism is so completely different that it has been necessary to adopt new ways of working (…). The advent of terrorist attacks designed to cause mass casualties, with no warning, sometimes involving the use of suicide, and with the threat of chemical, biological, radiological or nuclear weapons means that we can no longer wait until the point of attack before intervening. The threat to the public is simply too great to run that risk … the result of this is that there are occasions when suspected

terrorists are arrested at an earlier stage in their planning and preparation than would have been the case in the past."[17]

During the last decade, for instance, parliaments have been active in defining and adopting new offences in the "inchoate mode" and criminalising preparatory activities even if they are several steps away from the actual perpetration of the crime. Not only do inchoate offences expand criminal liability, but they also allow the use of enhanced preventive powers and police intervention before the commission of any substantive crime.

In relation to terrorism, additional tension arises between criminal justice, which is supposed to be impartial, and the politically charged concept of national security.[18] The risk of potential harm is often assessed on the basis of secret evidence and based on political considerations, possibly prior to the filing of a criminal charge. In cases of judicial review, this tension has sometimes led to a certain level of judicial deference towards the executive, which is perceived to be better placed to make decisions where national security is at stake.[19]

This paradigm shift towards preventive action poses critical challenges for the protection of individual rights. First, the boundaries of what constitutes dangerous behaviour are highly contentious, and problems arise with the assessment of future harm. Secondly, "suspicion" has replaced the more objective criterion of "reasonable belief" in most cases in order to justify police intervention at an early stage in terrorism cases, without the need to see evidence-gathering with a view to a prosecution. Governments can thus act on the lower standard of possibility of future harm rather than the higher standard of proof of past criminal activities. This allows a shift towards greater governmental discretion for reasons of national security at the expense of judicial scrutiny.[20] Lastly, preventive measures encompass a larger number of activities and affect a broader range of people. In fact, many powers are not explicitly limited in their scope to the terrorism context, international or otherwise. As a result of the disengagement of anti-terrorism legislation from a specific situation in time and/or space, the current policies have become applicable to a much wider range of circumstances. Whereas the use of ordinary powers implies a curtailment of the rights of a specific suspect, special powers/these kinds of agreements tend to affect more broadly the individual rights of all citizens, whatever risk he or she may (or may not) represent to the community.

Conclusions

In relation to preventive measures based on suspicion and risk-assessment procedures, serious dangers of dreadful injustice arise. Do governments really dispose of any means by which to assess whether an individual poses a risk to the public? Are they able to appraise the likelihood that an (otherwise only potential) harmful act will occur? What are the criteria to identify whether the measures adopted would effectively prevent an event from occurring? The question is also whether alternative ways of managing risk are possible.

The Stockholm Programme foresees the establishment in the area of Justice and Home Affairs of a comprehensive EU approach to the use of Passenger Name Record (EU-PNR) data for law enforcement purposes and the creation of a European framework for the communication of PNR data to third countries.

In 2007 already, the Commission made a proposal for a Framework Decision for a European PNR Agreement. It would create a coherent legal framework at the EU-level requiring airlines to transfer PNR information to law enforcement authorities for the purpose of preventing, investigating, and prosecuting terrorism and organised crime.[21] While increasing legal certainty, the new framework would also constitute an EU attempt to strike the right balance between privacy, security, and transparency. In addition, it would avoid unequal

protection of individual rights currently resulting from the many differences between existing PNR agreements with the US, Canada, and Australia. Moreover, the EU legal framework for the transfer of personal information to third countries will have to comply with the requirements of the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which was adopted on 30 December 2008, after several years of discussion. This instrument established a common level of privacy protection and a high level of security in the exchange of personal information throughout Europe and in the transfer of personal data to third countries.[22]

The entry into force of the Lisbon Treaty and the greater institutional involvement of the European Parliament have suspended the discussions on the establishment of an EU-PNR processing system. The plan is strongly supported by the Council and the Commission, but the negotiations will be complex due to the different approaches to privacy and data protection in the EU Member States. It is remarkable that, with the Lisbon Treaty, any PNR agreements require the consent of the Parliament before they can be concluded by the Council.

---

1. Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program ("Swift Agreement"), Council 11222/1/10 REV 1, 11222/1/10 REV 1 COR 1 and 11350/2/10.↩
2. The interim agreement had previously been rejected by the European Parliament in February 2010. The approval of the European Parliament became necessary following the entry into force of the Lisbon Treaty.↩
3. Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) and Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement).↩
4. Passenger Name Record is the general name given to elements gathered by airlines for each passenger journey, such as identification data (full name, date of birth and citizenship, sex, passport number and country of issuance), information on departure and return, billing and payment, services required.↩
5. See V. Papakonstantinou and P. de Hert, 'The PNR agreement and transatlantic anti-terrorism co-operation: no firm human rights framework on either side of the Atlantic', 2009, 46 CML Rev 885, pp. 892-898.↩
6. See, for instance, E. De Busser, Data protection in the EU and US criminal cooperation, Antwerpen, Maklu 2009; B. Siemen, 'The EU-US Agreement on Passenger Name Records and EC-Law: Data Protection, Competences and Human Rights Issues in International Agreements in the Community', 2004 German Yearbook of international Law 47, p. 629; Assemblée nationale, Rapport sur la proposition de decision cadre du Conseil relative à l'utilisation des données des dossiers passagers (Passenger Name Record, PNR) à des fins répressives, COM (2007) 654 final/n° E 3697, n°1447, 11 février 2009.↩
7. See, for instance, The Future of privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, 1 December 2009, 02356/09/EN, WP 168.↩
8. M. Mendez, "Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US", 2007 EuConst 3, pp. 127-147; G. Gilmore and J. Rijpma, 'Joined Cases C-317/04 and C-318/04', 2007 CML Rev 44, pp. 1081-1099.↩
9. In support of its judgment, the ECtHR refers back, mutatis mutandis, to its previous case-law: Kruslin v France, 1990, §§ 33 and 35; Rotaru v Romania, 2000, §§ 57-59; Weber and Saravia v Germany, 2008; Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria, 2007, §§ 75-77; Liberty and Others v UK, 2008, §§ 62-63.↩
10. Mandates for the renegotiation of these PNR agreements, as well as the one with the US have been adopted on 21 September 2010 in connection with Commissioner Malmström's idea of developing a "PNR package " with minimum requirements – mostly regarding data protection – for this type of agreements. The proposal for the PNR package was also adopted on 21 September.↩
11. See J. Lodge, 'Eu Homeland Security: citizens or suspects?', 2004 European Integration 26, 3, p. 253.↩
12. M.M. Feeley and J. Simon, 'The new penology', 1992 Criminology 30, 4, p. 449.↩
13. L. Zedner, 'Fixing the Future?' in S. Bronnit et al. (eds), Regulating Deviance, Oxford, Hart Publishing, 2008.↩
14. L. Zedner, 'Pre-crime and post-criminology?', 2007 Theoretical Criminolog, 11, p. 261.↩
15. Ibid, p. 262.↩
16. See E. Fisher, 'Precaution, precaution everywhere', 2002 Maastricht Journal of European and Comparative Law 9, p. 7. The analogy is made by Zedner, 'Fixing the Future?', 2008, pp. 187-88.↩
17. London Anti-Terrorism Branch (SO13), 'Submission in support of three month pre-charge detention' (2005), appendix of Home Affairs Committee, 'Terrorism Detention Powers' HC (2005-06) 910-I, 54 as quoted by J. McCulloch and S. Pickering, 'Pre-crime and counter-terrorism', 2009 British Journal of Criminology 49, 5, pp. 628-632.↩
18. McCulloch and Pickering, 'Pre-crime', 2009 (see footnote 16).↩
19. For instance, the House of Lords in the Belmarsh case (2004) had to consider whether sufficient evidence of a 'public emergency threatening the life of the nation' had been provided to justify the issue and continuance of the derogation notice under Art. 15 ECHR. The majority of the Court accepted that it was within the government's margin of appreciation to say that, after September 11, the terrorist threat amounted to a national emergency that could be said to threaten the life of the nation.↩

20. In this respect, it is significant to mention that Art. 16 of the Italian Law decree 144/2005 would have required the public prosecutor to obtain a specific authorisation from the Minister of Justice in order to proceed with the investigation of international terrorism offences. In order to avoid inappropriate interferences in what are meant to be independent judicial activities, Parliament has fortunately decided not to convert the controversial provision into law.↩
21. P. de Hert and V. Papakonstantinou, 'The EU PNR framework decision proposal: Towards completion of the PNR processing scene in Europe', 2010 Computer Law & Security Review26, 4, p. 368; M. Nino, 'The protection of personal data in the fight against terrorism', 2010, Utrecht Law Review, Vol. 6, 1, pp. 82-84.↩
22. On this instrument and other models of data protection in transatlantic cooperation, see E. De Busser, 'EU Data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?', 2010 Utrecht Law Review 6, 1, p. 86.↩

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union