§1. One of the major challenges for the current EU data protection regime is to ensure legal certainty. A series of interinstitutional conflicts and tensions have conveyed the image of a legislator that cannot be trusted, as not able or not willing to recognise the exact scope of the provisions it aims to establish. This issue concerns especially what Advocate General Léger has called in its Conclusions the “new set of issues” related to the “use of commercial data for law enforcement purposes,” which refers both to the PNR case and the Data Protection Case.

§2. From a legal point of view, however, the European Court of Justice (ECJ) has been clear in its judgement: the only factor to take into account in order to determine the scope of data processing is the nature of the processing itself, as opposed to the origin of the data. In this sense, the view manifested by the European Data Protection Supervisor according to which the judgement creates loopholes in EU legislation could be discussed. Indeed, all processing needs either to be included in the exemptions to Directive 95/46/EC, either to fall under the scope of the Directive.

§3. Despite the fact that such legal loopholes may not exist as such, it is undeniable that the “use of commercial data for law enforcement purposes” could require special protection provisions, different from those currently offered under the EU third pillar. Indeed, the collection of data for law enforcement purposes as commercial data could seriously mislead the data subject and damage therefore its individual rights.

§4. The will to enhance protection in those cases is precisely one of the reasons that have lead some EU institutional actors to privilege wide interpretations of the data processing falling under the EU first pillar. The first pillar offers, indeed, more consistent data protection, as well as other institutional specificities such a reinforced participation of the European Parliament and a less limited ECJ role.

§5. However, forced or creative interpretations of the scope of the Data Protection Directive contribute dangerously to the general lack of legal certainty already mentioned. In this sense, they do not serve the cause of effective EU data protection.

§6. Currently, one of the major differences between EU data protection in the first and in the third pillar is that in the latter there is no formal requirement to declare that a third country ensures ‘adequate’ data protection to allow the transfer of data to said country. The second version of the PNR agreement signed between the EU and the
US, approved in the framework of the third pillar, is nevertheless based on a Council Decision stating that ‘adequate’ protection will be provided by US authorities.

§7. The fact that such ‘adequate’ protection might indeed be provided is actually very strongly discussed, as well as probably impossible to prove. To the general difficulties already encountered by the EU to review such ‘adequacy’ for US processing falling under the first pillar, need to be added the specific review limitations related to security matters (such as, for instance, the possible use of the confidentiality principle to block checks coming from external authorities).

§8. If declaring that the US authorities offer ‘adequate’ data protection is not legally required (§6), allegedly not accurate and in any case subject to debate (§7), the interest for the Council to provide such a statement is doubtful.

§9. A very important lesson to be learned from the management of the PNR issue in the EU until now is the lack of efficiency of the European data protection Supervisory authorities in monitoring compliance with data protection law. By not taking any actions against airline companies not complying with data protection law, the data protection Supervisory authorities have shown what could be interpreted as a lack of courage. It is uncertain whether one needs to be disappointed by this. Rather it teaches us that the excellent work of the European data protection Supervisory authorities as privacy watch-dogs, may more often than one would expect, be in need of complementary political control and decision-making. To put it differently: data protection is one system of protection and action, but it would be a mistake to think that is a sufficient system on its own.

§10. The credibility of the current EU data protection system has also been undermined by the so-called ‘SWIFT case’, which also showed that serious violations of data protection law manage to escape from the supervision of the data protection authorities and finally need to be addressed at a different, political level. This can be linked to the general limitations of data protection law as legislation dominated by its procedural dimension, where priority is given to regulate inconvenient data transfers instead of avoiding them.

§11. Another actor with a capital role to play in the EU data protection regime is the judiciary, at least in theory. It bears the responsibility to proceed to the ultimate check of compliance of transfers with data protection principles from the human rights perspective. In this sense, Advocate Léger’s Opinion in the PNR case was dramatically unsatisfactory. It limited itself to a formal compliance check, instead of offering a strict review of the different alternatives encountered and their different impact on privacy and individual rights. In the era of continuous technology developments, the only way to judge proportionality and necessity of measures is via balancing the impact of choices.

§12. Another problem to be found in Advocate Léger’s Opinion in the PNR case is his non-acceptance of the capacity of the US to unilaterally modify the content of the PNR agreement. Indeed, Advocate Léger did not recognise such capacity and used the argument to dismantle part of the European Parliament’s argumentation. His interpretation on the question whether the provisions of the agreement are to be binding on the parties, or whether the US authorities are to be able to give a
unilateral explanation of how they intend to interpret them could nevertheless be different had he expressed his Opinion after the publication of the Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the USA, Concerning the Interpretation of Certain Provisions of the Undertakings Issued by DHS on 11 May 2004 in Connection with the Transfer by Air Carriers of Passenger Name Record (PNR) Data. The Letter seems to significantly change the factual background on which his Opinion is based and could serve to sustain that the parties are indeed allowed to substantially review how they intend to implement the agreement.

§13. Regarding the second and current version of the PNR agreement, a major aspect to be pointed out is the final provision according to which “This Agreement does not create or confer any right or benefit on any other person or entity, private or public”. This explicit denial of the data subject’s rights reinforces the idea that insisting on declaring that the protection provided by the US might be ‘adequate’ is not fully convincing.

§14. Concerning the question whether the EU has any realistic prospect of securing agreement on any provisions which the United States are reluctant to agree, it must be admitted that, if the second version of the agreement has not secured better protection than the first version, it is probably not realistic to expect any improvement in future agreements unless new approaches are adopted.

§15. Concerning the question whether the existing agreement with Canada can (with a change of legal base) be used as a model, it needs to be noted that dissimilarities between the US and Canada regarding data protection can be considered sufficient to require totally different approaches. The most notable dissimilarity is that Canada recognises the principle of the need of independent supervision, whereas the US does not.

§16. Taking into account the specificity of the use of commercial data for law enforcement purposes (§3), the weakness of data protection in the third pillar (§4), the apparent inopportunity of affirming the ‘adequacy’ of the protection ensured by the US authorities (§8), the limitations of the protection based almost exclusively on the supervision by data protection authorities (§10) and the unclear response to be expected from the judiciary (§11), it has to be recognised that there is an imperious need for the EU to establish new checks and balances in this field.

§17. New checks and balances should not be expected to come from the US side, neither should the responsibility for those checks and balances be placed by the EU exclusively on the hands of the US authorities, mainly because of the lack of accountability in case of non compliance. In this sense, the regulation of the duty to inform data subjects travelling from the EU on the data processed is a good example of what should be avoided in future agreements, as the duty is exclusively regulated by the Undertakings of the Department of Homeland Security Bureau of CBP, which can be unilaterally ‘interpreted’ by the US, and simply falls under CBP responsibility.

§18. For the sake of efficiency and accountability, checks and balances need to be implemented in the EU, under EU responsibility. The fact that the processing of the PNR is to take place in the US does not mean that the EU should simply rely on the
protection as promised by the US, without contributing to an effective protection inasmuch as possible.

§19. In the collection of data for law enforcement purposes as commercial data, information to the data subject is essential. Information on the further processing of the data must be given for two reasons: on the one hand, to ensure the possibility of the data subject to make effective use of its rights (notably, of rectification), and, on the other hand, to raise awareness of the current reality of data transfers to the general public. Both purposes are to be interpreted as part of the progressive empowerment of the data subject, which should be in fact the main objective to be fulfilled by the provision of information under EU law.

§20. The information given to the data subject should cover the exact data transferred, the moment when the transfer is expected to take place, the use foreseen after the transfer, and the exact rights the data subject has concerning the data once they have been transferred, as well as information on how to introduce requests to US authorities to use the rights recognised by the US and, suitably, contact information to EU Supervisory authorities able to offer assistance. The information should be provided at the moment of the collection, and therefore the obligation to inform should be placed on those responsible for the collection. Eventual complaints regarding costs of this measure should be forwarded to the US authorities responsible of implementing the data transfer system.

§21. The monitoring of this obligation could be taken care of by data protection authorities. Due to the European dimension of the issue, the monitoring should ideally be developed at EU level, or at least there should be mechanisms to coordinate actions. A EU level coordination of the monitoring could also contribute to the collection of information on eventual problems encountered by travellers, which could be used in future negotiations with the US. The possibility of offering assistance could be particularly useful in this sense, and would additionally contribute to increasing the quality of the data provided to the US authorities. The weight to be given in the negotiations to the view of the European data protection authorities could in the future substantially depend on the effective role they play in providing assistance to the data subjects to make sure the data transferred to the US and processed by US authorities is accurate.

§22. Better informed travellers represent not only data subjects effectively able to take benefit from the rights they have been recognised. Information is also instrumental to raise public awareness of the measures being implemented. Information is in this sense a key to the promotion of real public debate on data protection and data transfers, and therefore also an essential tool to enhance the role of parliaments.

§23. On a mid term perspective, other enhanced mechanism of protection should probably be established to reduce conflictive situations in the field of global data transfers. New paths to explore could include digital watermarking, an already widespread practice in the field of digital rights management allowing the marking of digital content. In fact, all the techniques used for Digital Restriction Management should be careful examined, as they can allow the secure transfer data that will be impossible to manipulate by non authorized parties, easy to track by the pertinent authorities and, more importantly, inaccessible after a certain number of processing
activities. This could be particularly useful in the search to a solution to the question on how information given can be restricted to the use for which it is given.

§24. The future PNR agreement needs imperatively to be approved only for a limited temporal application. Furthermore, it should include provisions on the elements to be taken into account for its own revision, notably: i) the analysis of the eventual persistent need for the transfer of data; ii) the examination of the practical utility of the transfers, inasmuch as demonstrated by practice; iii) the eventual concerns expressed by travellers, as monitored by data protection authorities; iv) technology developments that could improve the protection of data and/or enhance the enjoyment of individual rights related to the data transferred.

§25. In conclusion, regarding the position to be adopted by the Commission in the coming negotiations with the US, the major concern must be to conclude a temporary agreement subject to revision, whose main objective should be to effectively increase the level of protection of the individual rights with provisions to be implemented at EU level, and therefore accountable in the EU. Information to travellers is to be seen as a key element to empower the data subjects, to which data protection authorities should provide all the possible assistance.

§26. The part to be played by the European Parliament and national parliaments could be precisely to stand for this empowerment of the data subject, as a way to protect individual rights and promote public debate in the delicate field of the use of commercial data for law enforcement purposes.

This evidence was submitted on an individual (non corporate) basis and concluded 28th February 2007, in Brussels.