DRAFT PAPER – PLEASE DO NOT QUOTE

Transatlantic Transfer of Personal Data: Rebuilding Trust in EU-US Data Relations?

Juan Santos Vara
Professor of Public International and European Law
University of Salamanca
savajuan@usal.es

Soledad R. Sánchez-Tabernero
Doctoral Research Fellow in European Law
University of Salamanca
soledadrst@usal.es

Paper prepared for the Biannual Meeting of the European Studies Association, Boston, MA, March 5th-7th, 2015.

The present paper has benefited from the support of research project DER2012-36703, financed by the Spanish Ministry of Economy and Competitiveness.

1. Introduction

Transatlantic security relations are still characterized by the difficulty in finding a balance between the need to fight effectively against terrorism and organized crime, and the need to safeguard fundamental rights and, in particular, the protection of personal data. Since 29 March 2011, the European Union has been negotiating with the United States government an international framework agreement (the so-called 'Umbrella Agreement') in order to protect personal data transferred between the EU and the US for law-enforcement purposes. The NSA scandal further reaffirms the need to negotiate an Umbrella Agreement that ensures access for EU citizens to the US judicial system and a right to redress under the same conditions as US citizens.

Since the US is now willing to extend the right of redress to the EU citizens, it seems that one the main challenges affecting the negotiations have been resolved. The aim of this paper is to analyse to what extent the Umbrella Agreement contributes to striking a balance between the fight against terrorism and other serious crimes, and the protection of civil liberties and fundamental freedoms. This contribution will also assess

whether trust in the EU-US data flows has been rebuilt after the NSA scandal and the Parliamentary enquiry that has taken place in the EU.

The PNR and SWIFT Agreements fall within the scope of the current negotiations for an agreement between the EU and the US on the exchange of personal data in the framework of police and judicial cooperation in criminal matters.[1] On 3 December 2010, the Council authorised the opening of the negotiations for an agreement between the EU and the US on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters. This proposal was included in the Action Plan Implementing the Stockholm Programme.[2] The objective was to negotiate an umbrella agreement that would provide for a coherent set of data protection standards in the relations between the EU and the US. However, this agreement would not constitute the legal basis for any specific transfers of personal data. A specific legal basis for such data transfers would always be required. The conclusion of this agreement would only provide for a higher level of protection of personal data to the extent that it contained additional rules to the specific agreements on data transfer. It would also be required to ensure the effective application of data protection rules and their supervision by independent authorities. Unfortunately, the negotiations have advanced very slowly[3].

The access by US intelligence agencies to private data has seriously eroded transatlantic trust in the transfer of personal data. The negative impact that the NSA scandal had on transatlantic relations is further exacerbated by the lack of an effective judicial remedy for EU citizens under US law, particularly in cases of surveillance activities for intelligence purposes. Furthermore, the NSA scandal posed the need for genuine parliamentary oversight of the illegal surveillance activities developed by the American authorities, which could amount to an infringement of the SWIFT and PNR

[1] See European Commission, 'European Commission ready to start talks with US on personal data agreement to fight terrorism or crime', Press Release, 3 December 2010, available at

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661> (last visited 3 October 2013).

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-Delivering an area of freedom, security and justice for Europe's citizens-Action Plan Implementing the Stockholm Programme, COM(2010) 171 final.

[3] See S. in't Veld, 'Transatlantic Relations and security – Reflections from a Politician, Practitioner and Litigator', in E. Fahey & D. Curtin (eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US legal orders* (Cambridge University Press, Cambridge, 2014), pp. 237-245.

Agreements[4]. Since the inquiry into the American surveillance activities constituted an unprecedented test for democratic accountability in the EU, the Parliament had an excellent opportunity to enhance its role in transatlantic security relations. The LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens finished its report on January 2014 and the European Parliament adopted its resolution on March 2014[5].

This paper aims to analyse firstly, the extent to which the NSA scandal has damaged trust in EU-US transfer of data. PNR and SWIFT already raised serious concerns regarding breaches of data protection rights of EU citizens but the NSA scandal constituted the last straw in the already troubled waters of transatlantic data exchanges. While PNR and SWIFT are not the only existing data transfer agreements between the EU and the US, they are the most contentious. Secondly, this paper will try to examine whether the Umbrella Agreement can contribute to rebuilding trust in EU-US relations by laying down a sufficient and effective framework for data protection in the context of transatlantic cooperation. For that purpose, this paper will first look at the implications of the NSA scandal for trust in transatlantic data relations. Secondly, the challenges to transfers of data in EU-US relations will be examined, paying particular attention to weak level of protection in SWIFT and PNR as well as to their review process and issues of accountability. Thirdly, an analysis of the Commission's Non-Paper on the state of play of negotiations on the Umbrella Agreement will serve as a ground to assess whether the agreed proposals will provide sufficient safeguards against the identified concerns. Finally, provisional conclusions will be drawn on the basis of the current state of negotiations.

2. The Implications of the NSA Scandal for Trust in Transatlantic Data Relations

In June 2013, the press revealed that the US authorities had accessed and processed on a large scale the personal data of EU citizens using online serve providers. The EU institutions expressed serious concerns over PRISM and other such programmes implemented by the National Security Agency (NSA), since these

[4] 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 the purposes of the Terrorist Finance Tracking Program, *OJ* L 195, 27.7.2010, p. 5–14; Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJ* L 215, 11.8.2012, p. 5–14.

[5] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI))

initiatives could entail a serious violation of the fundamental rights of EU citizens and residents, and called on the US authorities to provide the EU with full information on such programmes.[6] The European Parliament opened an investigation into the matter in order to assess the impact of the US surveillance programmes regarding fundamental rights, in particular the right to respect for private life and communications, freedom of expression, the presumption of innocence and the right to an effective remedy. Some MEPs raised the possibility of suspending or even terminating the SWIFT and PNR Agreements during the hearings on the NSA surveillance programmes.[7]

The Parliament considered in its report that it has not been clarified whether US intelligence agencies have accessed SWIFT financial messages in the EU by intercepting SWIFT networks or banks' communication networks, alone or in cooperation with EU national intelligence agencies, and without having recourse to existing bilateral channels for mutual legal assistance and judicial cooperation.[8] Therefore, the Parliament asked the Commission to suspend the application of the TFTP Agreement. As regards the PNR Agreement, the Parliament expressed its concerns because the great majority of PNR data are saved in cloud systems operating on US soil under US law, which lacks data protection adequacy. It does not seem that the Commission and the Council are willing to suspend the application of the SWIFT and PNR Agreements, which constitutes a serious decision that could negatively affect transatlantic relations and, in particular, the negotiations on the Transatlantic Trade and Investment Partnership Agreement (TTIP).

The NSA scandal further reaffirms the need to negotiate a transatlantic framework agreement on the protection of personal data that ensures access for EU citizens to the US judicial system and the right to redress at the very least in the same conditions as US citizens.[9]

---

[6] See Commissioner Reding letter to the US Attorney General, Eric Holder, 10 June 2013; Statement by the President of the European Council, 11 July 2013; European Parliament resolution on the US National Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy, 2 July 2013.

[7] European Parliament, 'MEPs raise suspension of EU-US bank data deal', press release, 24 September 2013.

[8] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

[9] The access to justice and the redress system is very weak in the SWIFT and PNR agreements. See E. Fahey, 'Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress, and

3. Challenges to the Transfer of Data from the EU to the US

3.1. The weak protection of personal data in the SWIFT and PNR Agreements

Even though some of the concerns raised by the European Parliament as regards the 2009 SWIFT agreement found a satisfactory solution in the 2010 SWIFT Agreement, data protection provisions are not satisfactory[10]. There are no remarkable differences between the first and second SWIFT agreements. Since the European Parliament was involved during the negotiation process, it was more pleased to accept the second SWIFT compromise[11]. The Parliament was fully informed at all stages of the negotiations and its views were taken into account by the actors involved in the process.

The 2010 SWIFT Agreement is not fully satisfactory with respect to the protection of personal data. Firstly, the system is still based on the bulk transfer of data, because SWIFT does not technically allow targeted searches. The European Data Protection Supervisor (EDPS) held that 'the fact that the current SWIFT system does not allow a targeted search cannot be considered as a sufficient justification to make bulk data transfers lawful according to EU data protection law'.[12] The transmission of bulk data does not meet the proportionality and necessity requirements. Secondly, it is not acceptable that the Agreement allows keeping non-extracted data for five years. Thirdly, as regards judicial review, the Agreement explicitly states that the agreement 'shall not create or confer any right or benefit on any person or entity, private or public' (Article 18). The EDPS pointed out that 'this provision seems to annul or at least question the binding effect of those provisions of the agreement providing for data subjects' rights which are currently neither recognised nor enforceable under US law, in particular when data subjects are non US citizens or permanent residents'. In consequence, the provisions to protect the rights of EU citizens would not give access to any kind of judicial review in the US.

Remedies in EU-US Passenger Name Records and the Terrorism Finance Tracking Program', (2013) *Yearbook of European Law*, pp. 1-21.

[10] On the review of the implementation of the agreement, see S. in't Veld, *supra* note 3.

[11] See J. Santos Vara, 'Transatlantic counter-terrorism cooperation agreements on the transfer of personal data: a test for democratic accountability in the EU', in E. Fahey & D. Curtin (eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US legal orders* (Cambridge University Press, Cambridge, 2014), pp. 256-288.

[12] Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the 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, *OJ* 2010, C 355/12.

Similarly to the 2010 SWIFT Agreement, the new PNR Agreement provides stronger protection of EU citizens' right to privacy than the 2007 EU-US PNR Agreement. EU citizens will have the right to access their own PNR data and seek corrections, including the possibility of erasure or blocking, of his or her PNR data. However, the PNR Agreement concluded with the US is not satisfactory from the perspective of EU protection of fundamental rights. The most serious concerns were not removed. Firstly, the processing of PNR data is allowed not only for the purpose of preventing and prosecuting terrorism and serious transnational crimes. The data may also be used to investigate and prosecute 'other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature'.[13] Secondly, Article 4(2) allows for the use of PNR 'if ordered by a court'.[14] This clause would allow the use of PNR for any purpose, provided that it is ordered by a court. Thirdly, the 2011 PNR Agreement retains data almost indefinitely. The data shall be retained for an initial period of five years and then in a dormant data basis for a period of up to ten years. Following the dormant period, data retained must be rendered fully anonymised. Fourthly, even though the Agreement recognises that any individual may seek administrative and judicial redress in accordance with U.S. law,[15] it does not amount to admit a judicial redress equivalent to the right to effective judicial redress in the EU.[16] Article 21 explicitly states that the Agreement 'shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public'. Finally, it is not acceptable that data may also be used to ensure border security. According to Article 4(3) 'PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination'.

3.2. The review process of the PNR and SWIFT Agreements

[13] Justice and Home Affairs, Draft Recommendation on the draft Council decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security (17433/2011–C7-0511/2011–2011/0382(NLE)), 30 January 2012.

[14] PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court.

[15] Art. 13 PNR Agreement, *supra* note 4.

[16] See also the Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, *OJ* C 35, 9.2.2012, p. 16–22.

There are many review mechanisms in the PNR and SWIFT agreements concluded with the United States. The operation of the reviews of these two Agreements shows the weaknesses of governance in transatlantic security.[17] In order to understand the shortcomings presented by the accountability mechanism in the transfer of data from the EU to the US, it is crucial to briefly examine the main results arising from the periodic review of the of PNR and SWIFT Agreements.

Article 13 of the SWIFT Agreement provides for regular joint reviews of the safeguards, controls, and reciprocity provisions to be conducted by review teams from the EU and the US, including the Commission, the US Treasury Department and representatives of two data protection authorities from Member States. The review process may also include security and data protection experts and persons with judicial experience. The first joint review of the Agreement took place in February 2011 and covered the period of the first six months after the entry into force of the Agreement[18].

The EU review team concluded that the Agreement has been implemented in accordance with its provisions, including the data protection provisions. The EU recommended to give more public information on the way the program functions, in as far as this is possible, without endangering the effectiveness of the Program. The conclusions of the second review, that took place two years after the entry into force of the Agreement, were also very optimist[19]. According to the Commission's report, the implementation of the agreement has reached a very satisfactory level with also the EU increasingly profiting from it under the specific reciprocity arrangements.

As regards the third joint review that took place in April 2014, the Commission affirmed to be fully satisfied with the Agreement and with the proper implementation of its safeguards and controls.[20] The Commission pointed out that the consultations

[17] E. Fahey, *supra* note 9.
[18] Commission Staff Working Document Report on the joint review of the implementation of the 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 the purposes of the Terrorist Finance Tracking Program 17-18 February 2011, SEC(2011) 438 final, 30.3.2011.
[19] Commission Staff Working Document Report on the second joint review of the implementation of the 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 the purposes of the Terrorist Finance Tracking Program October 2012, SWD(2012) 454 final, 14.12.2012.
[20] Report from the Commission to the European Parliament and the Council on the joint review of the implementation of the 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 the purposes of the Terrorist Finance Tracking Program, COM(2014) 513 final, 11.8.2014.

conducted with the US after the NSA Scandal led to the conclusion that the US authorities had not obtained information from SWIFT outside of the TFTP Agreement. Therefore, the safeguards and controls included in the agreement were properly respected and implemented.

Europol is responsible for verifying whether the US request complies with the requirements of the Agreement, including the protection of personal data. It must be highlighted that the Agreement itself does not expressly contemplate the possibility that Europol should reject the transfer of data requested by the US, and indeed no transfer of data has as yet been rejected by Europol.[21] Europol has been heavily criticized for carrying out this role, but is a task that it did not ask to be responsible for and which is not clearly described in its mandate.[22] Within the field of data protection, the agency is subject to the Europol Joint Supervisory Body (EJSB).[23] The EJSB does not, however, have the capacity to block the transfer of unnecessary or disproportionate data to the US authorities. It must be pointed out that the European Parliament is not allowed either to supervise Europol intervention under the SWIFT Agreement.[24] The classification of this type of information as 'EU Secret' blocks any possibility for the Parliament to provide meaningful supervision of the implementation of the mandate conferred on Europol.

As regards to the 2011 PNR Agreement, Article 23 of provides for a joint review of its implementation one year after its entry into force (on 1 July 2012). The review was carried out in July 2013 by two teams represented, on the US side, by officials from the Department of Homeland Security (DHS) and, for the EU, by Commission officials and two Member State experts on data protection and law enforcement[25]. The report concluded that the operation of the agreement was satisfactory. It noted that DHS has an effective mechanism to filter out PNR data which have no clear connection to the US or which go beyond the categories of PNR data listed in the Agreement. The use of PNR data is consistent with the purpose limitations set out in the Agreement and 'follows an approach allowing [DHS] to maximise the added value of using PNR for law

[21] 'Europol JSB inspects for the second year the implementation of the TFTP Agreement', *Europol JSB Press Statement,* Brussels, 14 March 2012.
[22] European Parliament, *Parliamentary oversight of security and intelligence agencies in the European Union,* 2011, p. 46.
[23] Art. 34 of Council Decision of 6 April 2009 establishing a European Police Office (Europol), *OJ* L 121/37, 15.5.2009.
[24] See E. Fahey, *supra* note 9; J. Santos Vara, *supra* note 11.
[25] Joint Review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security, SEC (2013) 630 final, 27.11.2013.

enforcement purposes'. PNR data are held securely and subject to appropriate access controls. Although the Agreement authorises the use and processing of sensitive data 'in exceptional circumstances', this provision has not been used during the first year of operation of the Agreement, and internal DHS rules require the Commission to be notified within 48 hours if sensitive data are accessed. The report notes that the sharing of PNR data with other domestic (US) agencies or its onward transfer to other third countries remains limited. A further joint review will take place during the first half of 2015, followed by a formal joint evaluation of the Agreement in 2016.

The review process of PNR and SWIFT Agreements demonstrates that the shortcomings of governance in the transatlantic transfer of personal data are not yet overcome. All the signs are that the Commission has opted for facilitating the rebuilding of trust in the transfer of data to the USA within the framework of SWIFT and PNR agreements. Despite the fact that the NSA scandal made clear that the USA had very possibly accessed EU data protected by SWIFT and PNR outside the framework of these agreements, after the implementation review process carried out in 2014, the Commission has seemed fully satisfied.

4. The EU-US Umbrella Agreement: Much Ado About Nothing?

Many of the concerns raised by data protection deficits in transatlantic counter-terrorism relations and pointed out in this paper were supposed to be solved via the so called 'Umbrella Agreement' currently being negotiated by the EU and the US. The negotiations of this agreement started as a result of the mandate of the Council of 3 December 2010, authorising the Commission to open the negotiations, under Article 218(10) TFEU. Negotiations formally opened on 29 March 2011 and despite their slow pace are at the time of writing at an advanced stage, although some questions, particularly those regarding judicial redress for EU nationals in the US, remain contentious[26].

As it is concluded under Article 218(10) TFEU and under a substantive AFSJ legal basis, the European Parliament will play a key role in its conclusion. That is to be welcomed in light of the role that the European Parliament, and the LIBE Committee in particular, have played in the negotiations of SWIFT or PNR agreements, albeit at times

[26] EU-US Negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism, MEMO/11/203, Brussels, 29 March 2011.

lead more by its will to assert its influence in the conclusion of international agreements rather than to protect fundamental rights of EU citizens[27]. Particularly bearing in mind the relevance that digital rights had in the 2014 EP campaign, the EP could put the Commission under pressure in fighting for a stronger agreement with the possibility of rejection if the resulting Umbrella Agreement does not meet EU standards[28].

As has been previously mentioned, the Umbrella Agreement is not supposed to act as a legal basis for data transfer, for which other legal mechanisms are already in place. On the contrary, it aims to provide with a satisfactory solution for data protection in EU-US transfer of data for security purposes. It therefore aims 'to ensure a high level of protection of personal information and to enhance cooperation between the US and the EU for the prevention, investigation, detection or prosecution of criminal offences'[29]. Furthermore, this agreement would contribute to ensuring the coherence between EU-US counterterrorism cooperation and European values, currently challenged by the differences regarding data protection standards existing in the EU and the US[30]. Such a framework would be expected to lead to an overarching common understanding of privacy at the transatlantic level[31].

As has been pointed out previously in this paper, while the Parliament had been sufficiently involved in the negotiations leading up to the 2010 SWIFT Agreement and the new PNR Agreement, serious shortcomings as to the protection of personal data of EU citizens remained. Particularly, concerns were raised regarding SWIFT and PNR over retention periods, although they were notably striking in PNR. According to the Commission's Non-Paper, the concerns regarding retention periods could be solved through the establishment of 'specific retention periods' in order to ensure the requirements of necessity and appropriateness. To meet the requirement of appropriateness, the duration of retention periods shall take account of the purposes of processing or use, as well as the nature of the data and their impact on rights of the

[27] See J. Santos Vara, *supra* note 11, at 276.
[28] I. Brown, 'The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance', (2014) *International Journal of Law and Information Technology*, 1-18, at 13.
[29] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', 8761/14, Brussels, 09.04.2014, at 3.
[30] V. Mitsilegas, 'Transatlantic counterterrorism cooperation and European values: the elusive quest for coherence', in E. Fahey & D. Curtin (eds.), *A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US legal orders* (Cambridge University Press, Cambridge, 2014), pp. 289-315, at 312.
[31] *Ibid*.

individuals affected[32]. While the Commission praises those accomplishments, it is to be seen where specific retention periods will be laid down. Presumably, they would be enshrined in agreements granting legal basis for data transfers. Secondly, necessity and appropriateness remain rather broad concepts and open to interpretation. Rather or besides appropriateness, it would be preferable to see in the final text of the agreement an element of proportionality, as is the case of other instruments in the EU regarding limitations to data protection rights[33]. The principle of proportionality also includes an element of appropriateness insofar as it requires interferences to rights to '[1] be appropriate for attaining the legitimate objectives pursued by the legislation at issue and [2] do not exceed the limits of what is appropriate and necessary in order to achieve those objectives'[34].

Furthermore, while certain limitations on rights such as those found in the annulled Data Retention Directive tend to meet the necessity test, it is in the second strand of the proportionality test where they fail[35]. That is the case for excessive data retention periods, which is what is at issue here. It is to be hoped, nevertheless, that the lack of the proportionality element is just a drafting error in the Non-paper that will be corrected in the proposal submitted to the Parliament and the Council. Otherwise, the Parliament should not accept such a flagrant limitation of citizens' rights.

In view of the broad scope for interpretation of these concepts, it is understood that these requirements will only be effective if combined with adequate means of judicial review that enable an independent court or tribunal to scrutinise the interpretation of the administration, particularly since in view of the process of review of the SWIFT and PNR Agreements it appears that to the Commission the retention periods laid down in SWIFT and PNR are 'appropriate'[36]. Even then, it is rather likely that without further concretization in substantive agreements laying down the legal basis

[32] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', *supra* note 29, at 6.
[33] See recital 4 of the preamble in Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L 105, 13.4.2006, p. 54–63; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281 , 23/11/1995 pp. 31 – 50.
[34] Case C-293/12 and C-594/12, *Digital Rights Ireland*, judgment of the Court of 8 April 2014, nyr, para. 46.
[35] *Ibid.,* para. 69.
[36] See the Report on the joint review of the implementation of the SWIFT agreement, *supra* note 20, and the Joint Review of the implementation of the PNR Agreement, *supra* note 25.

for the transfer of data, necessity and appropriateness will be understood differently not only by the law enforcement authorities on each side of the Atlantic, but also by the judiciaries.

The SWIFT and the PNR Agreements involve the transfer of data of a broad quantity of individuals, not necessarily in connection with terrorism or a serious crime due to the system on which they are based (e.g. bulk transfer for SWIFT). This can be considered in light of the Court's ruling in *Digital Rights Ireland,* where it held that, concerning data retention periods, clear and precise rules governing the extent of the interference are required and it highlighted the fact that no distinction was made as to the categories of data regarding retention periods on the basis of the usefulness for the purposes of the objective pursued or according to the persons concerned[37]. The Non-Paper was issued just a day after the Court ruled on this issue. It is to be hoped that the Court's findings will be considered in the drafting of the proposal of the Umbrella Agreement on this point.

This latter point brings the debate to another troublesome element of the PNR Agreement: the fact that the processing of PNR data was allowed for other purposes than countering or preventing terrorism and other serious forms of transnational crime, but also for other crimes of over three years imprisonment which would be transnational in nature. In our view, those concerns will not be solved by the proposals included in the Non-Paper. In fact, both sides agreed that the 'umbrella agreement will cover personal data transferred for purposes of prevention, investigation, detection or prosecution of criminal offences'[38]. This is even broader than the terms included in the PNR data, which included the 3-year-plus requirement. This element is positive insofar as it will broaden the protection for all kinds of transfer of data for crime prevention purposes. It is also the purpose of concluding an Umbrella Agreement, as otherwise it would constantly need to be amended in order to broaden its scope should the need arise. However, it could in turn also lead to a new wave of agreements granting legal basis for transfer of data regarding petty crimes since decision-makers would understand that the Umbrella Agreement already provides sufficient guaranties.

[37] *Digital Rights Ireland*, *supra* note 34, paras. 63-66.
[38] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', *supra* note 29, at 4.

On this issue, the fact that the PNR data could be used for any purpose if ordered by a Court is to be recalled. In this sense, the Umbrella Agreement might shed some light and restrict this possibility insofar as it imposes a requirement of prior consent of the competent authority which originally sent the data in order to transfer it to a Third State or international organisation. Therefore, under the said provision of the PNR Agreement, transfers to Third States ordered by a Court for a different purpose could be covered, inter alia for migration-control purposes. Under the Umbrella Agreement, it appears that these hypothetical scenarios would be limited by a requirement of consent which should take account of the purpose for which the data was transferred and of whether the Third State or international organisation in question grants an appropriate level of protection[39]. Again, what an appropriate level of protection is in the terms of the Umbrella Agreement could be put into question.

On substantive principles of data protection, another element that questioned the necessity and proportionality of transatlantic data transfers was the transfer of bulk data justified by the fact that it was only possible to transfer bulk data under SWIFT. In fact, in light of *Digital Rights Ireland*, it is likely that should its concluding decision be taken to the Court of Justice via an action for annulment, it would be annulled on similar grounds. While the Non-Paper does not include substantive provisions on this question, it could be that the provisions on 'Automated Decision-Making' could have some relevance. Indeed, one of the problems raised by the transfer of bulk data, is that data of regular citizens would be transferred and they could be used for profiling. The same would be the case for profiling on the basis of PNR data retained for an almost indefinite period of time. These provisions therefore seem to provide some guarantees regarding decisions based on automated processing of information, such as profiling. However, whether these safeguards are sufficient in the eyes of the European citizen is also in question.

The Non-Paper states that as a matter of principle decisions negatively affecting the relevant interests of an individual cannot be adopted if they are based solely on automated processing of information[40]. This prohibition applies unless it is authorised by domestic law. In that case, decisions negatively affecting the relevant interests of an

[39] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', *supra* note 29, at 7.
[40] *Ibid.,* at 8.

individual could be based solely on an automated processing of information provided that 'appropriate safeguards are in place, including the possibility to obtain human intervention'[41]. A prohibition of this kind is certainly not sufficient to counter the pernicious effects of bulk transfers. If the discussed exemptions are added, the narrow scope of the prohibition can also be perceived. A requirement to be authorised by domestic law shows that the EU can leave data protection of EU citizens to the authorisation by US law. While the possibility of including human review is to be welcomed, it is not sufficient.

An important element of concern raised in the failed SWIFT agreement for the EU was raised by the differences between enforcement mechanisms under EU and US law. According to the EDPS, the US lacked an independent oversight mechanism[42]. An attempt to solving this issue, at least to some extent, was already included in the 2010 SWIFT agreement, and has been considered acceptable by the Commission in the review process of the SWIFT agreement[43]. This is also reinforced in the Non-Paper for the Umbrella Agreement, which requires effective oversight mechanisms. They shall put in place public authorities exercising independent oversight functions and powers, including investigation, intervention and review. They must be able to act upon complaints made by individuals relating to the measures implementing the agreement[44]. The Non-Paper takes account of the particularities of the US system but understands that a combination of supervisory authorities can cumulatively exercise the oversight functions entrusted to Data Protection Authorities in the EU. This combination of authorities is similar to that put in place for the SWIFT agreement and has been accepted by the Commission[45].

What is absent from the Non-Paper and where agreement has not been reached is the fundamental issue of judicial redress. As has been previously pointed out, many of the possible improvements can only be effective insofar as adequate means of redress are put in place, including the possibility of EU citizens to seek judicial review before US courts. There is already a theoretical possibility to seek judicial review under Article

[41] *Ibid.*
[42] EDPS, *supra* note 12, para. 36.
[43] V. Mitsilegas, *supra* note 30, at 301; Report on the joint review of the implementation of the SWIFT agreement, *supra* note 20, at 15.
[44] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', *supra* note 29, at 14.
[45] See Report on the joint review of the implementation of the SWIFT agreement, *supra* note 20, at 31-32.

13 of the PNR Agreement and Article 18 of the SWIFT Agreement, but the reality of this review is doubtful in view of the omission of the US Privacy Act of 1974 in these articles[46]. In this sense, before stepping down, Attorney General Holder agreed with Vice-President Reding on the Obama Administration's commitment towards seeking legislation that would give EU nationals the same rights that those granted to US nationals[47]. Commissioner Jurova has welcomed the US commitment and the proposal tabled for Congress, although is waiting to see the details of the proposal[48].

In absence of further information on the amendment to be proposed by the Obama Administration, the remarks by former Attorney General Holder, while they are to be welcomed, raise a number of concerns as to EU data protection standards. The proposed amendment seems to be based on equal treatment for EU and US nationals by granting redress for 'intentional or wilful disclosures of protected information', following the logic of the US Privacy Act 1974[49]. If this is to be implemented, EU citizens will enjoy the same possibilities of redress as US citizens. However, this would entail that, while enjoying judicial review to the same extent as US citizens, they would not enjoy the benefits derived from the agreement and thus would see their rights under the Charter of Fundamental Rights diminished[50]. What is particularly striking is that EU citizens would only be protected by the possibility to enjoy judicial review if the disclosure of their data by US agencies is 'intentional or wilful'.

It is true that the Non-Paper includes points on notification of data security incidents which requires appropriate action to mitigate the damage be promptly taken. This would call for a notification to the data provider and, '*where appropriate given the circumstances of the incident'* [emphasis added] to the individual concerned. Exceptions to this rule will be exhaustively listed and correspond to reasonable limitations,

[46] See E. Fahey, *supra* note 9, at 9-10, 13-15.
[47] Department of Justice, Office of Public Affairs, 'Attorney General Holder Pledges Support for Legislation to Provide E.U. Citizens with Judicial Redress in Cases of Wrongful Disclosure of Their Personal Data Transferred to the US for Law Enforcement Purposes', 25 June 2014.
[48] Commissioner Věra Jourová's remarks before the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee - 21 January 2015
[49] Department of Justice, *supra* note 47.
[50] Committee on Civil Liberties, Justice and Home Affairs, Working Document on future European Union (EU) – United States of America (US) international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters, 14.7.2014, p. 5.

according to the Non-Paper[51]. While this notification obligation encompasses other breaches than those being intentional or wilful, an obligation of notification is not sufficient in order to fulfil the EU requirements of data protection and sufficient means of administrative and judicial redress going further than cases of 'intentional or wilful' disclosures of data should be put in place. Whether the amendment of the US Privacy Act 1974 proposed by the Obama Administration will entail sufficient guarantees in this sense is to be seen. Otherwise, mutual recognition and mutual trust in countries where differences are so fundamental may be easier said than done[52]. Means of judicial review could in that case be established directly in the agreement, although this may not be adopted by US authorities.

Finally, another pending and quite relevant issue is whether the Umbrella Agreement, if finally adopted, will apply retroactively to transfers already performed under already concluded agreements. This is a key element to the rebuilding of trust in transatlantic data relations in view of the possible breaches of data transfer agreements operated as a result of the PRISM programme that lead to the NSA scandal. Besides, it would be particularly relevant with respect to judicial review, especially since as has been pointed out both the SWIFT (Article 18) and PNR Agreements (Article 21) state that these agreements shall not create or confer any right or benefit on any person or entity, private or public. If the Umbrella Agreement applied retroactively, then the impossibility of claiming direct effect of SWIFT and PNR before a court of law could be solved by applying the Umbrella Agreement.

5. Concluding remarks

The analysis of the review process of PNR and SWIFT Agreements can lead to the conclusion that demonstrates that the flaws in the transatlantic transfer of personal data are not yet overcome. In spite of the scandalous NSA revelations which showed a high possibility that the USA had accessed SWIFT and PNR data in breach of the agreement, the Commission has seemed fully satisfied. It therefore appears to have opted for

[51] Non-Paper on State of play of negotiations on EU-US data protection 'Umbrella Agreement', *supra* note 29, at 9.
[52] V. Mitsilegas, *supra* note 30, at 313.

facilitating the rebuilding of trust in the transfer of data to the USA within the framework of PNR and SWIFT agreements.

The Umbrella Agreement has been perceived as a key step for rebuilding trust in transatlantic transfer of data for law enforcement purposes after the NSA scandal. The agreed principles found in the Non-Paper of April 2014 show certain improvements to the main concerns as to data protection of EU citizens outlined in the most contentious data-transfer agreements between the EU and the US (namely, SWIFT and PNR). Having sketched the main challenges found in those agreements, it can be concluded that some improvements are found, inter alia in the limitations to transfers of data to third countries and international organisations or to automated-decision making. However, there is still a certain gap to reach EU data protection standards.

An element of proportionality regarding data protection periods should be included and combined with judicial review. Besides, in light of the ruling in *Digital Rights Ireland*, it is submitted that differences in data retention periods should be included, particularly when data are transferred in bulk. Data of individuals not related to law-enforcement purposes should not be subject to the same data retention periods as those linked to it. Furthermore, nothing in the Non-Paper provides sufficient guarantees to the broad scope of purposes for which PNR data can be used.

Finally, the fundamental question lies in judicial redress. The effectiveness of the improvements found in the Umbrella Agreement depend on whether EU citizens have effective means of judicial protection available, not only for intentional and wilful disclosure of information but also for other breaches of the administration. Whether this will be achieved remains to be seen, as remains whether mutual trust can be rebuilt after the NSA scandal. While the Commission may seem willing to reach an agreement with US authorities, the Parliament may and should be tougher if it wants to assert itself as a credible defender of fundamental rights of its electorate rather than as a schoolboy craving for a lead role at the Christmas play of external decision making.