Retos y oportunidades del

Entretenimiento en línea

Actas del VIII Congreso Internacional Internet, Derecho y Política
Universitat Oberta de Catalunya. Barcelona, 9-10 Julio, 2012

Challenges and Opportunities of

Online Entertainment

Proceedings of the 8th International Conference on Internet, Law & Politics
Universitat Oberta de Catalunya. Barcelona, 9-10 July, 2012

COORDINADORES

Agustí Cerrillo i Martínez, Miquel Peguera
Ismael Peña-López, María José Pifarré de Moner,
Mònica Vilasau Solana

UOC Universitat Oberta de Catalunya

HUYGENS EDITORIAL

Retos y oportunidades del entretenimiento en línea

Actas del VIII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 9-10 de julio de 2012

Challenges and Opportunities of Online Entertainment

Proceedings of the 8th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 9-10 July, 2012

2012

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL

RETOS Y OPORTUNIDADES DEL ENTRETENIMIENTO EN LÍNEA

CHALLENGES AND OPPORTUNITIES OF ONLINE ENTERTAINMENT

La Costa, 44-46, át. 1ª
08023 Barcelona
www.huygens.es

ISBN: 978-84-695-4123-4
Impreso en España

Índice General

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y JUEGO ONLINE

PNR AND SWIFT AGREEMENTS. EXTERNAL RELATIONS OF THE EU ON DATA PROTECTION MATTERS

Cristina Blasi Casagran
European University Institute

ABSTRACT: Since the 9/11 attacks there has been a dramatic increase in measures adopted in order to prevent and to combat international terrorism, which has had an impact on the existing data protection framework within the EU.

This study will focus on the analysis of the international agreements signed between the EU and third countries regarding data transfers. In particular, PNR Agreements as well as the SWIFT Agreements will be examined, and I will also analyse the interconnection between the internal and external dimensions in depth, focusing on their mutual impact.

In order to do this, an analysis and comparison of the current EU-US PNR Agreement, EU-Australia PNR Agreement and EU-Canada PNR Agreement will be carried out first. After, I will study the future European PNR Directive and possible implications for current PNR Agreements.

I will then examine SWIFT and SWIFT II Agreements, paying special attention to the enhanced powers of the EP. At this point, it will be necessary to study the European Terrorist Finance Tracking System project as part of the EU Internal Security Strategy.

Finally, concerning the negotiations recently opened by European Union and the United States on an agreement to protect personal information exchanged in the context of fighting crime and terrorism, I will examine this potential international agreement on data transfers between the EU and the US, and its impact on the rest of international agreements with regard to data protection.

KEYWORDS: Data protection, international agreements, PNR, SWIFT, TFTS.

1. INTRODUCTION

The terrorist attacks on September 11, 2001 led directly to the increased number of measures taken by the US authorities and consisting of the collection, processing and storage of personal data in order to prevent and combat international terrorism. These counter-terrorism measures has had an impact on the existing data protection framework within the EU. In particular, closer cooperation between the US and the EU has become a priority, resulting in frequent dialogue and contact between their respective officials in order to harmonise police, judicial and border control policy matters. Thus, many international agreements on border security and criminal matters have been signed between the EU and third countries since 2001, and data protection has come to occupy a key sticking point of such agreements. Therefore, this study will analyse the international agreements signed between the EU and third countries regarding data transfers, looking in depth at the mutual impact of the internal and external dimensions. In particular, it will examine the PNR Agreements and the SWIFT Agreements.

In order to do so, first, the current EU-US PNR Agreement, EU-Australia PNR Agreement and EU-Canada PNR Agreement will be compared and analysed. Subsequently, but still as part of the first section, I will study the future European PNR Directive and possible implications for current PNR Agreements. Second, I will then examine SWIFT and SWIFT II Agreements, paying special attention to the enhanced powers of the European Parliament (hereinafter, EP). At this point it will be necessary to study the European Terrorist Finance Tracking System (hereinafter, TFTS) project as part of the EU Internal Security Strategy. Finally, I will study the recent negotiations for a new US-EU Framework Agreement on Data Protection, an its impact (if any) on current and future international agreements on data transfers, aiming to harmonise both legal orders in the field of data protection matters.

This study is presented as an attempt to disclouse the great external influences (especially from the US) that the EU has been subject to with regard to counter-terrorist measures since 9/11 attacks. However, before starting the analysis of the existing international agreements on data transfers concluded between the EU and third countries, it is worth summarizing in the next section some key issues on data protection with respect to third countries.

2. KEY ISSUES OF DATA TRANSFERS TO THIRD COUNTRIES

When the European Communities adopted the first Directive on data protection in 1995,[1] its *rationale* was to lay down data transfers among Member States as a result of the internal market established since the Maastricht Treaty. Thus, the free movement of goods, persons, services and capital brought an increasing flow of personal data from one Member State to the other, which needed to be regulated within the European territory.

However, both recent technological progress (with the consolidation of the use of Internet) and current global security measures have had an impact on the processing of personal data. Thus, cross-border flows of personal data soon spread beyond European borders as well as beyond pure commercial interests. Accordingly, the market place has undergone an enormous digitalisation in the last twenty years, in which online purchases have increased significantly. This means that not only companies within the EU process personal data in a commercial transaction, but also industries based outside the European borders can easily collect, process and store data from EU citizens.

Regarding data transfers to third countries, the current[2] Directive of 1995 foresees the possibility of carrying out international transfers for commercial reasons. Yet, considering that before the Treaty of Lisbon only the European Communities were empowered with the legal personality necessary to conclude international agreements, that Directive was the one

1 OJ L 281 , 23/11/1995 P.31-50

2 This is the current EU Data Protection Directive at the time this paper is written. However, proposals for a Regulation and a Directive were launched by the Commission on 25th January 2012, and they are being deliberated upon by the EP. See COM(2012) 10 final and COM(2012) 11/4 draft, 25.01.2012.

used as a legal basis to sign international agreements on data transfers. Regarding the requirements to carry out the international transfer, according to article 25.1 of the Directive 95/46/EC, *«The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection»* (Emphasis my own).

According the paragraph 6 of the same article, the general rule is that the Commission has the competence to decide whether the third country guarantees this adequate level of protection or not.[3] However, in absence of the recognition by the European Commission of such adequacy, Data Protection Authorities (hereinafter, DPAs) can determine that a data transfer to third countries is lawful by implementing art. 26.2 of the Directive 95/46/EC. This provision foresees that *«a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights»*. In that situation, considering that the particular third country does not afford *a priori* an adequate level of data protection, the DPA will require a standard application form before performing the transfer, to which is attached a copy of the agreement between the data exporter and the data importer.[4] In that sense, the Commission Decision 2002/16/EC of 27 December 2001[5] was adopted in order to facilitate the transfer of personal data from a data controller established in the European Union to a processor established in a third country which does not offer adequate level of protection. This Decision was repealed in 2010 by the Decision 2010/87/EC,[6] which updated the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection. This legal framework enabled the Commission to sign the first Passenger Name Record (hereinafter, PNR) Agreement, as will be discussed below.

3. PASSENGER NAME RECORD AGREEMENTS

In response to the 9/11 attacks, US authorities adopted measures that obliged airlines taking off, landing or flying through US territory to turn over all their flight booking and

3 For instance, adequate standards has been recognised by the Commission to Argentina, Canada, Switzerland and US, among others.

4 Grigore-Octav Stan and Georgiana Ghitu. «Cross-Border Transfer of Personal Data. The Example of Romanian Legislation», Chapter 17 of *Personal Data Privacy and Protection in a Surveillance Era. Technologies and Practices.* Edithor: Christina Akrivopoulou & Athanasios Psygkas. IGI Global; Hershey PA (USA) 2010, p.309.

5 OJ L 6, 10.1.2002, p. 52.

6 OJ L 39, 12.2.2010, p. 5-17.

departure data to the US government. This information is referred as «*Passenger Name Record*» (PNR) data.

With respect to EU, the Commission has signed three PNR Agreements to date: one with the US, another with Canada and a third one with Australia. Regarding the EU-US PNR Agreement, it was signed pursuant to Art. 25 of Directive 95/46/EC. This agreement was a direct consequence of a US law adopted in November 2001,[7] under which any airline with flights taking off or landing within the US territory was obliged to provide the Bureau of Customs Border Protection (hereinafter, CBP) with electronic access to their PNR data.[8] The EU, in an effort to avoid conflicts between the US law and the existing EU data protection standards, signed a PNR agreement with the US in 2003. Thus, after the US guaranteed an adequate protection of passenger data,[9] the Community adopted Commission Decision 2004/535/EC[10] and Council Decision 2004/496/EC,[11] necessary to execute the international agreement.

On the subject of the chosen legal basis, as mentioned above, the agreement was based on the Directive 95/46/EC, falling thus under the scope of ex-art. 95 TEC (former first pillar). However, the EP, supported by the European Data Protection Supervisor (hereinafter, EDPS), appealed that the Decisions be annulled before the CJEU. The EP argued that the EU-US PNR Agreement had been adopted under the wrong legal basis since it was not an issue concerning an internal market, but rather a matter of public security and criminal law (third pillar). The Court agreed, and in May 2006, annuled both Decisions because it was found that the matter related closer to public security than commercial activity.[12] To explain its ruling, the Court opined *«While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature.[...][T]hat decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes».*[13] Consequently, the agreement was annulled as well.

Thereafter, a second PNR Agreement[14] was adopted in October 2006, although it was only provisional. This time the agreement fell under the scope of the third pillar and was

7 U.S. Aviation and Transportation Security Act, Pub.L. 107–71, 115 STAT. 597, 19.11.2001

8 Aviation and Transportation Security Act (ATSA), 19 November 2001 (Public Law 107-71, 107th Congress, 49 USC Section 44909(c) (3) (2001))

9 Undertakings of the Department of Homeland Security, Customs and Border Protection. Retrieved from http://www.dhs.gov/interweb/assetlibrary/CBP- DHS_PNRUndertakings5-25-04.pdf

10 OJ L235, 06.07.2004, p.11.

11 OJ L183, 20.05.2004, p.83.

12 C-317/04 , 30.05.2006. OJ C 178, 29.07.2006, P.1

13 *Ibid*. par.57

14 OJ L 298, 27.10.2006, p. 29-31.

concluded between the EU and the US, culminating with the Council Decision 2006/729/CFSP/JHA.[15] As noted above, international agreements on data transfers signed under the basis of the first pillar had to comply with the «adequacy principle» (Art. 25 Directive 95/46/EC) .This was not the case, however, when they fell under the scope of the third pillar, where each Member State applied its own standards. Therefore, while airline companies' concerns of infringing data protection legislation were solved with this new agreement; new concerns arose within the EU, since the new agreement did not require «adequate» data protection in international transfers.

Regarding the question of who carried out the negotiations, the former art. 24.1 TEU established that, *«When it is necessary to conclude an agreement with one or more States or international organisations in implementation of this title the Council may authorise the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect.»* The Council thus decided on a mandate for the negotiations and authorised the Presidency and the Commission to negotiate on behalf of the EU.[16]

The second PNR Agreement expired on 31 July 2007 and was immediately replaced by the third and current[17] EU-US PNR Agreement.[18] This third Agreement was signed and provisionally applied in July 2007 through the Council Decision 2007/551/CFSP/JHA.[19] However, it has never been formally concluded because of the position of the EP,[20] which has never given its consent to the proposal of the Agreement drafted by the Commission.[21]

The entry into force of the Treaty of Lisbon has given new competences to the EP, which is now required to give consent before concluding any international agreement, according to Article 218 (6) TFEU. Hence, in May 2010, the EP responded to the request on the existing PNR agreement with the US postponing its vote because the agreements did not meet the minimum requirements on data protection.[22] This fact made it necessary to draft a new PNR Agreement between the EU and the US, which was proposed by the Commission

15 Council Decision 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, 13226/06, 11.10.2006.

16 EU/US Passenger Name Record (PNR) Agreement, House of Lords, European Union Committee, 21st Report of Session 2006–07 p.27.

17 At the time this article is written, this is the current agreement. However, a new PNR agreement is expected to come into force in the coming months.

18 OJ L 204, 4.8.2007, p.18-25.

19 OJ L 204, 4.8.2007, p.16-17.

20 European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA(2010)0144.

21 COM(2009)702 final, 17.12.2009.

22 P7_TA(2010)0144, 05.05.2010.

in November 2011,[23] and was approved by the EP[24] and the Council[25] in April 2012. The agreement will most likely enter into force in the coming month.[26]

However, as mentioned above, the PNR agreement between the EU and the US was the first but not the only one. In fact, the EU has also PNR agreements with Australia and Canada, and the number of PNR ageeements might increase in a near future, since bilateral negotiations on new PNR agreements with other third countries are currently ongoing. Therefore, it is essential that all these PNR agreements are consistent among them; yet, comparing the three existing PNR agreements, many divergences between them can be noted, as will be analysed below.

First, let us look at the number of data elements requested from the airline companies. The EU-US PNR Agreement (hereinafter, US PNR) offers the most reduced amount of data collected with an attached list of 18 different items. This list has one less data element than the 2007 PNR agreement and definitely much less than the 34-element list included in the first PNR agreement between the EU and the US, in 2004.

The 18-element list in US PNR is also lower than the list of 25 elements annexed in the EU-Canada PNR Agreement[27] (hereinafter, Canada PNR), which was launched in 2005 but never adopted. Likewise, the US PNR has one fewer elements than the new EU-Australia PNR Agreement[28] (hereinafter, Australia PNR), which as in its first agreement with the EU in 2008, has maintained the number of requested elements at 19.

Concerning the data retention periods, the US PNR keeps passenger data the longest, with a retention period of 10 to 15 years (15 years only in the case of terrorists). However, the US authorities justify such a long period by stating that data would only be available in an active database for the first six months, removing afterwards all names, so that data become «depersonalised» by five years. After five years, data would be transferred to a «dormant database», and there kept up to 10-15 years from its collection. In contrast, Canada PNR foresees a retention period of three and a half years, which could be increased up to six years if a person is under investigation. The Australia PNR establishes a period of five and a half years, which ultimately is the same time span stipulated in its first PNR agreement in 2008, albeit that agreement set out a period of retention of three and a half years, with the possibility to extend it two further years when necessary.

---

23 COM/2011/0807, 23.11.2011.

24 P7_TA-PROV(2012)0134, 19.04.2012.

25 9186/12, PRESSE 173, 26.04.2012.

26 *Ibid.*

27 OJ L 82, 21.3.2006, p.15; Adequacy Decision: OJ L 91, 29.3.2006, p. 49.

28 Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, 10093/11, 13.09.2011.
http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/11/324&format=HTML&aged=0&language=EN&guiLanguage=fr

Finally, with regard to the transfer method used, the three PNR agreements prescribe the «push method», a process by which airline companies collect PNR data in their databases and then transfer such data to the respective government authorities. The push system is a sign of progress in respecting data protection rights, considering that in the first and second US PNR Agreements (2004 and 2006) the transfer method was always based on the «pull method». Under the old pull method, the US authorities had access to all data in airline companies' databases; consequently, data was collected and processed under US law, with no regard for EU data protection law. This practice changed with the US PNR in 2007, which made the pull method the alternative when a push method was not possible. With the push method in force, this now means that the processing of data is collected by EU airlines first (which later will be transferred to US authorities) must be in full compliance with the EU data protection legislation. Canada, on the other hand, applied a push method from the beginning, in its first PNR agreement in 2005; and even though Australia did not define it clearly in its first agreement of 2008,[29] the push method is expressly stated in its current PNR agreement with the EU, in force since 2011.

Parallel to the current divergence among the EU PNR agreements with third countries, the EU has launched a proposal for a EU PNR Directive. With this proposal the EU aims to regulate PNR data according to the EU legal framework. The next section discusses the scope and purposes of this Directive.

4. EU PNR DIRECTIVE

Some MEPs have been voicing their concern about the lack of reciprocity on PNR matters: with these international agreements data flows are basically transferred from the EU to the US, but not vice versa. Therefore, along with the negotiation of PNR Agreements, the possibility to create a PNR scheme within the EU has been under discussion since 2007, when the Commission launched a Proposal for a Council framework Decision[30] with the aim to «*harmonise Member State's provisions on obligations for air carriers operating flights to or from the territory of at least one Member State regarding the transmission of PNR data to the competent authorities for the purpose of preventing and fighting terrorist offences and organised crime.*»

More than three years later, in February 2011, the Commission presented a Proposal for a PNR Directive to be adopted by the EP together with the Council,[31] this time under the legal basis of the Treaty of Lisbon,[32] which enhances the competences of the European

29 Agreement between Australia and the EU on the processing and transfer of the EU-sourced Passenger Name Record data by air carriers to the Australian costumes services, 30.06.2008 (OJ L 213, 8,82008, p.49).

30 COM(2007) 654 final, 06.11.2007.

31 COM(2011) 32 final, 2.2.2011.

32 Articles 82(1)(d) and 87(2)(a) TFEU.

institutions. Thus, the Commission stated that the Proposal of Directive was in line with art. 8 of the Charter of Fundamental Rights and the art.16 TFEU, along with the Council Framework Decision 2008/977/JHA.[33]

The proposal was divided into two parts: An explanatory memorandum, where the Commission pointed out the grounds and context and development for the Proposal; and the Proposal as it should be adopted by the EP and the Council, containing twenty articles vis-à-vis the rules concerning PNR transfers.

In the memorandum, the Commission introduced the objective of its Proposal noting the aim of creating a European area of freedom, security and justice and stressing the necessity to establish a harmonised scheme to collect PNR data among EU Member states. The Commission based its Proposal on the recent increase of transnational terrorism as well as the impact of current measures on programmes such as SIS, SIS II, VIS and the Stockholm Programme. Subsequently, the Commission referred to the existing provisions within the EU as border management tools, API, SIS and VIS, highlighting that there would be no interference with the current border controls within the EU, since PNR data is *«used as a criminal intelligence tool rather than as a border control tool»*. The Commission also noted coherence between the Proposal and the Communication of 21 September 2010 'On the global approach to transfers of Passenger Name Record (PNR) data to third countries'.

Regarding the contents of the Proposal of the Directive, its purposes are the prevention, detection, investigation and prosecution of terrorist offences, serious crimes,[34] and serious transnational crimes. In this sense, the Commission put forward a retention of 19 different PNR data for period of time not exceeding five years, although the data must be «anonymised» after a very short period of 30 days. The Commission also emphasises that *«The collection and use of sensitive data directly or indirectly revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life, is prohibited»*.

As in all existing PNR agreements, the Proposal suggests a push method (and not a pull method), in which Member States would not have direct access to the carriers' IT Systems. The text also suggested the establishment of an independent national supervisory authority responsible for advising and monitoring how PNR data is processed as well as a national Passenger Information Unit (PIU) to protect data, which latter would deal with statistical information on PNR data (art. 18 of the Proposal).

Art. 8 of the Proposal is of particular interest, since it foresees that a Member State may only transfer PNR data and the results of the processing of PNR data to a third country on a case-by-case basis. This requirement would be in accordance with the recent PNR Agre-

33 *Op.cit.* COM(2011) 32 final, p.8.

34 Pursuant to Article 2(2) of Council Framework Decision 2002/584/JHA, punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State

ement with Australia (Art. 19.1 of the Agreement), whereas the EU-US PNR Agreement does not mention any case-by-case requirement in its Article 17 on «Onward Transfer».

It remains to be seen what will happen with this PNR Directive, and whether it will finally be approved by the Council and the Parliament. It was proposed by the Commission in February 2011, but no, more than one year later it is still stuck in the EP. In contrast, the EU-US PNR Agreement was proposed eight months later, and EP has already voted in favor of it. it has already been voted by the EP. Hence, it seems that an agreement on the external PNR schemes was foregoing the internal dimension of the EU PNR Directive.

Moreover, it is presently an open question regarding how the existing PNR internacional agreements will interact with the Directive. In this respect, if the Directive is finally adopted as it is proposed today, it could produce at least two results for passengers that fly from Europe to the US: i) such passenger would have 18 PNR collection items transferred to the US, but 19 in the EU database; or ii) such collected passenger PNR data would be retained for 15 years in the US and only 5 years in the EU.

Lastly, despite the new PNR Directive having the objective of preventing 27 divergent national systems,[35] it could paradoxically create additional fragmentation between EU data protection laws and those in third countries. Consequently, the mutual impact between the internal and external PNR regulatory frameworks will be of a greater interest in the times ahead, as such impact could determine the EU's position and level of influence regarding data processing matters.

5. SWIFT AGREEMENTS

Since September 11, 2001, there has been exchange of financial data between the US and the EU. In fact, in December 2001, two US – Europol agreements were concluded to facilitate the exchange of information related to global financial movements.[36] They were part of the so-called Terrorist Finance Tracking Program (hereinafter, TFTP), originally a secret Program uncovered in 2006 by the New York Times.[37] The Program, which was created by the Bush administration after the 9/11 attacks as an antiterrorist measure, in the beginning consisted in the US authorities pulling data from the private company *Society for the Worldwide Interbank Financial Telecommunication* (hereinafter, SWIFT) on EU citizens, without any involvement

35 Some Members States, such as UK or Belgium, have already their own PNR systems.

36 «Agreement Between the United States of America and the European Police Office», December 6, 2001, at https://www.europol.europa.eu/sites/default/files/flags/united_states_of_america.pdf; «Supplemental Agreement Between the Europol Police Office and the United States of America on the Exchange of Personal Data and Related Information,» December 20, 2002. https://www.europol.europa.eu/sites/default/files/flags/supplemental_agreement_between_europol_and_the_usa_on_exchange_of_personal_data_and_related_information.pdf

37 Eric Lichtblau and James Risen, «Bank Data Is Sifted by U.S. in Secret to Block Terror», *The New York Times*, June 23, 2006. http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all

of the EU, since this company was based in Belgium but had servers located in US territory. Even though SWIFT had to comply with Belgian national law implementing Directive 95/46/EC (first pillar), in order to avoid potential clashes of its practices with the European law, the company always processed EU citizens' data through its servers located in the US. Later, however, the fact that SWIFT servers moved completely to European territory[38] made impossible to avoid European privacy concerns, and the Commission urged to draft an Agreement enabling such data transfers from the EU to the US, because it was clear that the purpose of this cross-border transfer was not commercial but for criminal matters.

Consequently, on 30 November 2009, under the legal basis of the former Art. 24 and Art. 38 TEU, the EU and the US signed the first official SWIFT Agreement, exactly one day before the Lisbon Treaty came into force. This event had important consequences.[39] The agreement was provisionally applied on 1 February 2010 and was supposed to be applied temporarily until 31st December that same year. However, the legal basis to conclude international agreements changed with the Treaty of Lisbon and so too did the powers of the EP: From the Treaty of Lisbon, the Council can only adopt a decision authorising the conclusion of the agreement after obtaining the consent of the EP.[40] Thus, on 11 February 2010, the EP rejected the adoption of SWIFT Agreement, arguing a lack of protection of personal data.[41] After the EP withheld its consent with regard to SWIFT, the Commission received a mandate by the Council to restart negotiations with the US authorities with the aim of composing a new draft agreement (SWIFT II).[42] The new text was approved for a five-year period by the Council and this time also by the EP in July 2010.[43]

Nevertheless, even this new SWIFT agreement between the EU and the US has been controversial. The EDPS pointed out in an Opinion[44] that the bulk transfer of personal data should be replaced by a filtering mechanism in the EU, transferring only relevant and necessary data to the US and that the retention period of five years was too long. Likewise, the EP[45] raised concerns in March 2011, since Europol, which is in charge of checking US

38 Marise Cremona, « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena, p.13; and Deirdre Curtin «Top Secret Europe», *Universiteit vvan Amsterdam*,p.6.

39 For a more exhaustive analysis of the facts, see, Cremona M, « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena., 11-13; and Curtin D. M, «Top Secret Europe», *Universiteit vvan Amsterdam*, 2011.

40 Article 218 (6) TFEU.

41 P7_TA(2010)0029.

42 Council of the European Union, 11575/10 PRESSE 194, 28.06.2010.

43 A7-0224/2010, 05.07.2010.

44 OJ C 355, 29.12.2010, p.10.

45 Press release, «SWIFT implementation report: MEPs raise serious data protection concerns», Committee on Civil Liberties, Justice and Home Affairs, March 2011.

compliance with the agreement, did not provide any updated-written information about the requests from the US Treasury Department and its compliance with European data data protection standards. The dispute on document secrecy between the Council and the EP ended up on 4 May 2012 when the CJEU ruled in favour of the EP document requests[46]. The Council argument about the «negatively impact on the European Union's negotiating position» did not convince the Court, since the Council had «not established the risk of a threat to the public interest». Thus, the CJEU decision will probably increase the EU transparency rules in the negotiation of international agreements[47].

Moreover, as in PNR schemes, the interdependence of internal and external objectives[48] on data processing within the scope of the AFSJ had an impact on the subsequent data protection legislation within the EU with regard to financial data, as will be examined in the next section.

6. CREATION OF EU TFTS

The SWIFT II Agreement included two additional changes. The first was Commission's appointment of an independent observer based in Washington D.C., and the second was the future creation of an EU program equivalent to the US TFTP.

Considering this last condition, the EU is currently negotiating its own European Terrorist Finance Tracking System (hereinafter, TFTS), which would run parallel to the current US TFTP. In July 2011, the Commission launched a Communication called «A European terrorist finance tracking system: available options».[49] In it the Commission pointed out that *«the possible establishment of a system for extracting the data on EU territory would have consequences for the existing EU-US TFTP Agreement…[which] would need to be adjusted if the European Union decides to establish such a system.»* According to art. 72 TFEU, which states that the EU cannot affect the responsibility of its Member States on issues regarding «*the maintenance of law and order and the safeguarding of internal security»,* the Communication contained different available options for the EU and its TFTS,[50] which will have to be debated by the Council and the EP. In particular, the Commission proposed three possible TFTS. In the three of them the safeguards and controls would be centralised, but data pro-

46 T-529/09 - In 't Veld v Council, 04.05.2012.

47 FOX, B (2012), «Commission pushes for document secrecy despite court judgement», *EUObserver.com,* 08.05.2012. Retrieved from http://euobserver.com/22/116181

48 CREMONA M (2011) «The External Action in the JHA Domain: A Legal Perspective» in *The External Dimension of the Area of Freedom, Security and Justice*, ed. M. Cremona, J. Monar, S. Poli (Brussels: Peter Lang, 2011), 6.

49 COM(2011) 429 final, 13.7.2011.

50 The first option would be the creation of a EU TFTS coordination and analytical service, the second an EU TFTS extradition service, and the third would be a Financial Intelligence Unit coordination.

viders are still undefined, since it would probably include many companies and not only SWIFT, unlike the current SWIFT Agreement.

Moreover, the Commission is unclear about whether it would be more convenient to establish the system in the form of an «EU central TFTS Unit» or, instead, a Financial Intelligence Unit (FIU) Platform. The latter would suppose a higher involvement of the Member States, since this platform would be composed of all FIUs of Member States.

Furthermore, the Commission leaves open the role of this system, proposing three different options: The first would consist of managing the search results, so that the requests would be at a EU level; on the contrary, the system could also have a more limited role, only distributing searches to the Member States, which would be the ones in charge of the requests; and finally the Commission foresees, in the case of the FIU Platform, the possibility of handling citizens' requests as well as conducting searches. These searches would be verified either at the national or the EU level.

In addition, it is not yet clear whether the key bodies of the system would be the current Europol[51] and Eurojust, or, in the case of the FIU Platform, FIUs and national authorities would constitute the institutional structure. Finally, the legal basis for this EU TFTS is still undefined, but it would not be surprising that it is the same proposed in the PNR Directive, namely, Art. 82(1)(d) and Art. 87(2)(a) TFEU.

Whatever the scope and nature of this system turns out to be, the Commission points out that it is to be seen as positive, since it would contribute to limiting the amount of personal data transferred to the US (limiting the transfer of bulk data to the US). Nevertheless, the Art. 29 WP reacted against this Communication in September 2011,[52] saying that it is not entirely clear how this aim of limiting the data to be transferred would be met. In particular the Art.29 WP noted that the Communication refers to collection of the so-called «raw data», which in fact, if the data minimisation principle is not complied with, could be considered as «bulk data». Moreover, the Art. 29 WP argues that there is no evidence that the processing of personal data with regard to the EU TFTP is necessary, proportionate and legitimate as a remedy for the shortcomings of current US-TFTP.

Likewise, this EU TFTS project, as part of the EU Internal Security Strategy, is presented by the Commission as an attempt to prevent the transnational transfer of certain data belonging to European citizens to US authorities, so that the external regulation of collection and storage of financial data according to SWIFT II will have to be adapted to this new EU framework, constraining the collection and transfer of data according to the levels

51 However, the EDPS (Opinion June 2010), the EP (Press release March 2011) and the Art. 29 WP (Letter September 2011) have already raised concerns about the independence of Europol in the processing and transfer of personal data.

52 Letter from Article 29 Data Protection Working Party to Commissioner Cecilia Malmström. Subject: Terrorist Finance Tracking System (TFTS) – European Commission Communication COM (2011) 429. 29.09.2011.

of necessity and proportionality. However, the Art. 29 WP has already stated that it will be difficult to continue the existing US-TFTP parallel with the establishment of the EU TFTS.

Finally, as with the above-mentioned future impact between the EU PNR Directive and the current PNR agreements, the compatibility of the EU TFTP with the SWIFT II Agreement will be of great importance. Will this European program follow the existing external scheme on financial data transfers? Or rather, will the European model establish the parameters to amend the current SWIFT agreement? It is still too early to answer this question; however, if the future EU TFTS has a stronger impact on the SWIFT II, it could solve the current lack of transparence in the transfers to the US territory. Additionally, it could offer higher data protection standards when EU financial data is transfered beyond European borders.

7. STEPS FOR THE US-EU FRAMEWORK AGREEMENT ON DATA PROTECTION

As the number of international agreements on data transfers between the EU and the US has increased significantly in the last ten years, many attempts have been made to reach a general adequacy framework on data protection between them. However, while Washington wants an umbrella agreement in which the EU would largely accept US data privacy standards as adequate, and thereby making the negotiation of future data-sharing accords easier,[53] the EU is willing to make the US amend its privacy laws so that they comport with the EU data protection legal framework.

The EP launched the first call for this agreement in March 2009.[54] One year later, in May 2010, the Commission drafted a mandate on the negotiation terms,[55] which the Council authorised on 3 December 2010.[56] Negotiations officially commenced in March 2011.[57] Since then, several meetings have taken place between the Commission and the US authorities.[58] Furthermore, in November 2011, the EU and the US pledged in a joint statement to finalize negotiations on a comprehensive US-EU data privacy and protection agreement.[59]

---

53 Kristin Archick, *«U.S.-EU Cooperation Against Terrorism»*, Congressional Research Service, May 2, 2011, p.10.

54 OJ C 117 E, 6.5.2010, p.198-206.

55 IP/10/609.

56 See Commission press release on http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1661.

57 MEMO/11/203, 29.03.2011.

58 To date, sessions have been held on 5-6 May, 26 May, 24 June, 28 July, 9 September, 9 November, 13 December 2011 and 13 February 2012. See European Commission, JUST/C3/MHB D(2011), 31.01.2012.

59 MEMO/11/842, 28.11.2012. The same idea was also reminded in MEMO/12/192, 12.03.2012.

With regard to the content of the agreement, the US authorities have been leading the negotiations, highlighting their preferences in terms of data retention, «transfers onwards», data breach notification, sensitive data, and liability and proportionality rules. In this respect, the US has taken a position against establishing specific data retention periods, suggesting that such periods should be decided in accordance with each parties´ domestic law.[60] As regards data breach notifications, the US considers that only *serious* breaches should be notified, while the Commission has supported the notification of data breaches in all cases, excluding certain exemptions.[61] In addition, the US appears reluctant to transpose the High Level Contact Group's (HLCG) principle of *proportionality*[62] in the agreement, arguing that this term is foreign to US data protection law, and that such a principle could produce unknown effects.[63] Finally, the Commission is pushing to get that individuals have a real possibility to obtain administrative and judicial redress, establishing enforceable legal provisions.[64]

Although the EU and the US view the Agreement´s adoption as a long-term goal, the truth is that it is currently taking shape at a time where many changes are occurring in the area of data processing. In particular, there have been recent moves from both the US and the EU legal orders in order to align their data protection in some respects. For instance, on 25 January 2012 the Commission proposed a European Data Protection Package, composed of a General Data Protection Regulation and a Police and Criminal Justice Data Protection Directive.[65] Later, the White House launched a White Paper on a future «Consumer Privacy Bill of Rights» on 22 February 2012.[66] This Bill lays down the basis for a federal US legal framework on data privacy, which currently falls under sectoral legislations. Only time will tell how a future EU-US data protection agreement will interact with both the US and the EU internal data protection legilations.

On the subject of the material scope of the agreement, it has been agreed by both the Commission and the US authorities that the agreement itself will not be the legal basis for any transfers of personal data, and that a specific legal basis for such transfers will always be required.[67] Consequently, the future general agreement will probably not be prioritised

60 European Commission, JUST/C3/MHB D(2011), 31.01.2012.

61 *Ibid.*

62 About HLCG principles, see http://www.statewatch.org/news/2008/mar/eu-us-dp-principles.pdf

63 JUST/C3/MHB D(2011), Op.cit. For further information about the HLCG, see Mary Ellen Callahan, «New International Privacy Principles for Law Enforcement and Security», retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_new_int_privacy_principles_law_enforcement_security.pdf

64 REDING V, SPEECH/12/316, 3.05.2012, p.8.

65 COM(2012) 10 final and COM(2012) 11/4 draft, 25.01.2012.

66 White House, «Consumer Data Privacy in a Networked World: A Framework for Protecting and Promoting Innovation in the Global Digitally Economy. February 2012. Retrieved from: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

67 European Commission, JUST/C3/MHB D(2011), 31.01.2012.

over other more specific EU-US international treaties dealing with data processing matters. Moreover, the US has already stated that the new agreement will not be applicable to cases where data are collected by private parties and afterwards processed by law enforcement authorities for security purposes.[68] In PNR and SWIFT agreements the private parties involved (i.e., air carriers and the Belgian bank SWIFT) collect personal data for EU internal market purposes, but then, they transfer them to the US authorities for preventing and combating terrorism. Accordingly, the impact of this future agreement on current PNR and SWIFT agreements with the US might be very small (or even non-existent).

Thus, only at first sight the future US-EU data protection agreement could result in the most successful legislative tool for establishing common minimal standards on data protection between both the EU and US. However, the fact that the US has already constrained the scope of the Agreement to specific law enforcement purposes makes one wonder what the real impact of the Agreement will be.

8. CONCLUSION

From the foregoing discussion, we can see that there has been a clear evolution regarding the European external competence to legislate data protection. Originally, the Community was competent, enjoying implied powers to negotiate internal market issues beyond the European borders.[69] However, the increase of international terrorism has compelled the EU to adopt new international agreements on data transfers such as PNR Agreements and SWIFT Agreements. Thus, since the 9/11 attacks and the terrorist attacks in Madrid and London in 2004 and 2005, there has been a progressive shift in the purposes of processing personal data from the commercial reasons (former first pillar) to the aim to adopt criminal measures (former third pillar). This has had implications for the applicable legal basis to conclude international agreements, since it was no longer the Community that was competent to conclude international agreements on data flows regarding criminal matters, but the EU.

At the same time, these new international agreements have pushed the EU to amend its own internal legislation on data protection, in order to solve the problems of legal basis stemming from the confusing structure in pillars and its blurred division depending on whether the purpose of processing data is commercial or for security reasons.

Given the prevalence of these PNR and SWIFT agreements, it is clear that the EU security policy could benefit from additional structural coherence between its internal and external aspects. Not only have there been divergences, but fragmentations concerning data protection laws have also occured among EU Member States, as well as between the EU and other third countries. In response to these controversies, since the Treaty of Lisbon the protection of personal data in the EU has enjoyed unprecedented status, which has been

68 *Ibid.*

69 Following ERTA-Doctrine.

reflected through subsequent proposals by the Commission: the EU PNR Directive and the EU TFTS. Both proposals aim to legislate *internally* issues that have already been legislated *externally* for years.

Moreover, in seeking to strike the balance between the protection of personal data, on the one hand, and data processing for security purposes, on the other, the EU and the US are considering the adoption of a EU-US data protection agreement. However, so far it is difficult to see what impact this future umbrella agreement will have on the existing EU-US deals, such as PNR and SWIFT. Although the future EU-US data protection agreement is announced as an attempt to bring the European and American legal orders closer, it is unclear what the scope and implications of this agreement will be.

Regarding the interplay between the European and international perspectives in terms of data processing, to date the US legislation has undoubtly been the main influence on EU internal legislation and international agreements on this field. It is true that the European institutions (especially the EP) have been leading the promotion of individual data protection; yet, necessity and the external pressures for the EU to cooperate in a transatlantic counter-terrorism framework are too strong. Hence, as it has been recently seen with the EP aproval of the new EU-US PNR Agreement, the EU, in some cases, is willing to prioritise security over the EU fundamental right of data protection.

9. BIBLIOGRAPHY

Cremona M. (2011) «The External Action in the JHA Domain: A Legal Perspective» in *The External Dimension of the Area of Freedom, Security and Justice*, ed. M. Cremona, J. Monar, S. Poli (Brussels: Peter Lang).

Callahan M.E (2010) «New International Privacy Principles for Law Enforcement and Security», *The Privacy Advisor,* The Official Newsletter of the International Association of Privacy Professionals (IAPP), January 2010 Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_new_int_privacy_principles_law_enforcement_security.pdf

Cremona M. (2011), « Justice and Home Affaires in a Globalised World: Ambitions and Reality in the tale of US-EU SWIFT Agreement», *Institute for European Integration Research,* Working Paper nº 04/2011, Viena

Cremona M. (2010), «Disconnection Clauses in EC Law and Practice» in *Mixed Agreements Revisited - The EU and its Member States in the World*, eds. C Hillion and P Koutrakos (Oxfort: Hart Publishing, 2010).

Curtin D. M (2011) «Top Secret Europe», *Universiteit vvan Amsterdam*.

Laja S. (2012), *UK joins EU deal to share air travellers' data with US*, TheGuardian, 01.03.2012. Retrieved from http://www.guardian.co.uk/government-computing-network/2012/mar/01/home-office-pnr-agreement-eu-us?INTCMP=SRCH

Lichtblau E., Risen J. (2006), «Bank Data Is Sifted by U.S. in Secret to Block Terror», *The New York Times*, June 23, 2006. Retrieved from

http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all

Pérez Francesch J.LL, Gil Márquez T. and Gacitúa Espósito, A. (2011) «Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represeivos o preventivos?» Institut de Ciències Polítiques i Socials, UAB. Working Paper 297, Barcelona.

Reding V. (2011) «Stronger data protection rules at EU level: EU- Justice Commissioner Viviane Reding and German Consumer Protection Minister Ilse Aigner join forces», MEMO/11/762, November 07, 2011.

Reding V. (2011) «Building trust in the Digital Single Market: Reforming the EU's data protection rules», SPEECH/11/814, November 28, 2011.

Stan, G.O. and Ghitu, G. (2010), «Cross-Border Transfer of Personal Data. The Example of Romanian Legislation», Chapter 17 of *Personal Data Privacy and Protection in a Surveillance Era. Technologies and Practices.* Edithor: Christina Akrivopoulou & Athanasios Psygkas. IGI Global; Hershey PA (USA).

Worth D. (2011) *EC wants all non-European business to adhere to Data Protection Directive*, v3.co.uk, November 08, 2011. Retrieved from http://www.v3.co.uk