RANKED AMONG THE WORLD'S TOP 10 THINK TANKS
CEPS Liberty and Security in Europe
CENTRE FOR EUROPEAN POLICY STUDIES

Made in the USA? The Influence of the US on the EU's Data Protection Regime

November 2009

Patryk Pawlak

Abstract

Recent developments have shown that the EU's border security policy is greatly influenced by the US. This influence simultaneously has implications for other EU policies, including those on data protection. This paper highlights that policy-making at the transatlantic level is increasingly taking place through informal networks, such as the High-Level Political Dialogue on Border and Transportation Security and the High-Level Contact Group on data protection, which allow US involvement in EU policy-making. This tendency stems from the growing personal relationships among policy-makers, the gradual substitution of formal instruments with less formal contracts and informal understandings shaping the content of formal agreements. Drawing from empirical examples of EU–US cooperation on data protection in the context of homeland security, the paper analyses the repercussions of these developments and the issues that remain unresolved, and offers policy recommendations.

ISBN 978-92-9079-946-7
Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

MADE IN THE USA? THE INFLUENCE OF THE US ON THE EU'S DATA PROTECTION REGIME

CEPS LIBERTY AND SECURITY IN EUROPE/NOVEMBER 2009

PATRYK PAWLAK*

1. Introduction

In recent years, the issues of data protection and privacy have dominated much of the transatlantic agenda. The discussion started with the controversial transfer of passenger name record (PNR) data to the US Customs and Border Protection and ensued over the use of SWIFT data for the fight against terrorism.[1] Currently, the EU and the US are considering a way forward, including the conclusion of an EU–US international agreement on data protection. Such an agreement would have significant consequences for the EU data protection system and the daily life of EU citizens. The latest Commission proposal for the next multi-annual programme for the Area of Freedom, Security and Justice (the Stockholm Programme) states explicitly that "the work on data protection conducted with the US could serve as a basis for future agreements".[2] Therefore, it is both timely and necessary to reflect on the possible shape of the EU data protection regime. In this context, it is also worth exploring the evolution of EU–US relations from having an antagonistic character to a converging one. Although several authors have addressed the far-reaching implications these measures pose for EU citizens and third-country nationals,[3] many issues still call for systematic study.

The objective of this paper is to examine the role the US plays in the development of the border policies of the EU. Towards that aim, it investigates the processes underlying transatlantic cooperation in the field of personal data transfers for security purposes. The paper argues that the influence of the US in these EU policies has strengthened the prevailing role of the US as an agenda-setter and the emergence of new actors and informal networks at the transatlantic level. The consequent learning process has resulted in increasing trust and the build-up of personal relationships between EU and American policy-makers. This process has not only made the EU more open towards American policies, but has also led to the development of similar solutions in other EU affairs.[4]

---

* Patryk Pawlak is a researcher at the European University Institute in Florence and a member of the Transatlantic Post-Doc Fellowship for International Relations and Security (TAPIR). The author is grateful to Sergio Carrera and the anonymous reviewer for their comments and suggestions on earlier drafts of this paper.

[1] See Y. Moiny, *Protection of personal data and citizens' rights of privacy in the fight against the financing of terrorism*, CEPS Policy Brief No. 67, CEPS, Brussels, March 2005. Criticism of these policies was expressed, among others, by Peter Hobbing in *Tracing Terrorists: The EU–Canada Agreement in PNR Matters*, CEPS Special Report, CEPS, Brussels (revised version), 17 November 2008.

[2] European Commission, Communication on an Area of Freedom, Security and Justice serving the citizen, COM(2009) 262 final, Brussels, 10 June 2009.

[3] See for instance, E. Guild, S. Carrera and F. Geyer, *The Commission's new border package. Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No 154, CEPS, Brussels, March 2008.

[4] See J. Argomaniz, "When the EU is the 'norm-taker': The Passenger Name Records agreement and the EU's internalisation of US border security norms", *Journal of European Integration*, Vol. 31, No. 1, 2009, pp. 119-136. For more about the theoretical underpinnings of this paper, see P.S. Ring and A.H.

2. Towards a transatlantic smart border?

The strategy of 'smart borders' presented by the White House in 2002 assumed that "[t]he border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory".[5] To that end, the advanced technology was applied "to track the movement of cargo and the entry and exit of individuals, conveyances, and vehicles".[6] The implementation of this policy was pursued in several ways, including the expansion of the US-VISIT Programme to new areas or most recently through the establishment of the Electronic System of Travel Authorisation (ESTA). The US-VISIT Programme was conceived in 1996 as a tool to help identify visa over-stayers. It was re-launched after the terrorist attacks of 2001 to include travellers' biometric information (i.e. digital fingerprints and a photograph), with the objective of checking them against a watch list of known criminals and suspected terrorists. The use of PNR information was meant to further improve this capability and to help identify connections between travellers on the same flight who might belong to the same terrorist group. Similarly, the ESTA system is a new pre-travel authorisation programme for travellers from visa-waiver countries. The information submitted is checked against several law enforcement databases before a person's departure. The purpose of this new tool is to mitigate security risks associated with the travel of persons who have the nationality of visa-waiver countries.

The US response came to be perceived as not just "re-bordering" with enhanced border controls physically located between states[7] but as leading to the emergence of wide zones of virtual, transnational border-control practices that span the globe.[8] As Guild (2003) concluded, the border took on "a new sacred symbolism as the line of security".[9] Effective border controls that did not undermine international trade and legitimate travel could not be achieved without globally implemented instruments.[10] Since the Bush administration considered international mechanisms too time-consuming and potentially ineffective,[11] they opted for the unilateral adoption of laws. Because of

---

Van De Ven, "Developmental processes of cooperative interorganisational relationships", *Academy of Management Journal*, Vol. 19, No. 1, 1994, pp. 90-118.

[5] The White House, *Smart Borders for the 21st Century*, Office of the Press Secretary, Washington, D.C., 25 January 2002(a) (retrieved from http://usinfo.state.gov/is/Archive_Index/Border_Security_Smart_Borders_for_the_21st_Century.html).

[6] Ibid.

[7] See P. Andreas, "Re-bordering of America after 11 September", *Brown Journal of World Affairs*, Vol. 8, No. 2, 2002, pp. 195-202; see also P. Andreas, "Redrawing the Line: Borders and Security in the 21st Century", *International Security*, Vol. 28, No. 2, 2003, pp. 78-112; and also M.B. Salter, "At the Threshold of Security: A Theory of Borders", in M.B. Salter and E. Zureik (eds), *Global Surveillance and Policing: Borders, Security, Identity*, New York: Willan Publishing, 2005, pp. 36-50.

[8] See R. Koslowski, *International cooperation to create smart borders*, Woodrow Wilson International Center for Scholars, Washington, D.C., 2004; see also M.B. Salter, "Borders, Passports, and the Global Mobility Regime", in B.S. Turner (ed.), *Handbook of Globalization Studies*, London: Taylor and Francis, 2009. For a criticism of such an approach, see D. Bigo, "Globalized (in)Security: The Field and the Ban-opticon", in D. Bigo and A. Tsoukala (eds), *Terror, Insecurity and Liberty*, London: Routledge, 2008, pp. 10-48.

[9] E. Guild, "International terrorism and EU immigration, asylum and border policy: The unexpected victims of 11 September 2001", *European Foreign Affairs Review*, Vol. 8, No. 3, 2003, p. 345.

[10] S.E. Flynn, "Beyond Border Control", *Foreign Affairs*, Vol. 79, No. 6, 2000.

[11] Derived from interviews with US officials, Washington, D.C., March–July 2007. About 74 face-to-face interviews were conducted from October 2006 to February 2009, as a part of doctoral research. The interviewees were representatives of the EU institutions, the US administration, non-governmental organisations and research institutes. All of the interviewees agreed to be quoted as a part of this research in exchange for being granted anonymity.

their extraterritorial character and broad implications for civil liberties,[12] many of those measures provoked disagreements of a legal and political nature, especially in the EU.[13] For instance, measures like the ESTA were criticised with concerns that "security management is shifting from a state-based perspective to a more individual-based focus".[14]

The transnational nature of the US homeland security regulations and their coercive mechanisms (such as fines or the refusal of landing rights for air operators in the case of PNR transfers) compelled the EU to adjust its policies in line with those of the US. The enhanced cooperation between EU and American officials that developed on the occasions of numerous bilateral contacts eventually led to the EU embracing some normative principles underlying the policies of the US. The use of personal information for security purposes and the protection of such information became the most controversial and debated issues in transatlantic relations. Some of the major points of divergence stemmed from differences in approaches to the treatment and transmission of personal information. In the EU, the system of data protection derives from rules in Continental law and it frames the right to privacy as one of fundamental human rights. The US, on the other hand, treats personal information as a commodity and the right to privacy is protected by common law mechanisms.

Despite numerous differences, the EU and US advanced their cooperation on data exchange. A series of bilateral agreements has been concluded, including the EU–US PNR Agreements of 2004, 2006 and 2007,[15] the Europol–US Agreement of 2002,[16] and the SWIFT Agreement of 2007.[17] Furthermore, the discussion about border protection in the EU increasingly resembles that at the transatlantic level. It is now recognised that "migratory pressure, as well as the prevention of entry of persons seeking to enter the EU for illegitimate reasons, are obvious challenges facing the Union".[18]

---

[12] See E. Guild, "The judicialisation of armed conflict: Transforming the twenty-first century", in J. Huysmans, A. Dobson and R. Prokhovnik (eds), *The politics of protection, sites of insecurity and political agency*, London: Routledge, 2006; D. Bigo, S. Carrera, E. Guild and R.B.J. Walker, *The changing landscape of European liberty and security: Mid-term report on the results of the CHALLENGE project*, CHALLENGE Research Paper No. 4, CEPS, Brussels, February 2007; A. Tsoukala, *Security, Risk and Human Rights: A vanishing relationship?*, CEPS Special Report, CEPS, Brussels, September 2008.

[13] In 2004, Pat Cox, the president of the European Parliament, stated that "[w]hile naturally accepting that the US Administration is perfectly free to exercise its sovereign right to protect its own homeland, both the EU and the US must guard against a new form of creeping extra-territoriality" (Cox, 2004).

[14] European Parliament, *Data protection from a transatlantic perspective: The EU and US move towards an international data protection agreement?*, PE 408.320, DG for Internal Policies of the Union, Brussels, October 2008, p. 30.

[15] See Council of the European Union, Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20.05.2004; see also Council of the European Union, Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204, 04.08.2007(a).

[16] Council of the European Union, Consolidated version of the Draft Supplemental Agreement between the United States of America and Europol on the exchange of personal data and related information, 15231/02, Brussels, 5 December 2002.

[17] Council of the European Union, Processing of EU-originating Personal Data by United States Treasury Department for Counter-Terrorism Purposes – 'SWIFT', 10741/2/07 REV 2, Brussels, 29 June 2007(b).

[18] European Commission, Communication on preparing the next steps in border management in the European Union, COM(2008) 69 final, Brussels, 13 February 2008.

The border package presented by the European Commission[19] proposes a number of measures similar to those adopted in the US. For instance, third-country nationals subject to the visa obligation are already verified in conjunction with their visa application, but in the future they will be checked against the Visa Information System, which entails biometric information. In addition, all persons travelling to the EU by air will be checked through their advanced passenger information. Other new tools currently debated include facilitation of border crossing for bona fide travellers, introduction of an extry/exit system and establishment of an ESTA.

Among all these developments, two deserve particular attention: a) the discussion of a potential, international, data protection agreement between the EU and the US and b) the establishment of the EU PNR system. While the former exemplifies the progress in EU–US cooperation, the latter shows clearly the extent to which the EU's internal security policies are influenced by the instruments previously adopted in the US.

2.1 The EU–US PNR Agreements

In the US, the 9/11 National Commission Report stated clearly that "targeting travel is at least as powerful a weapon against terrorists as targeting their money. The US should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility".[20] To that effect, the 2004 Intelligence Reform and Terrorism Prevention Act called on the Department of Homeland Security (DHS) to establish mechanisms that would allow a comparison of "passenger information for any international flight to or from the US against the consolidated and integrated terrorist watch-list maintained by the Federal Government before departure of the flight".[21] On the basis of the Aviation and Transportation Security Act of 2001, the US requested all airlines arriving to or departing from US airports to submit PNR data. To ensure greater compliance, it was established that airlines failing to comply could be fined up to $6,000 per passenger and lose landing rights.

The American legislation in question undermined the EU data protection laws, in particular the EU's Data Protection Directive of 1995, which constitutes the backbone of EU activities in this area.[22] According to Art. 25 of the Directive, any transborder transfer of personal information is only allowed if it has been decided that the third country provides an "adequate level of protection" in terms of the standards applied in the EU.[23] Since no such decision had been taken regarding the US data protection system,[24] any transfer of passenger data should be considered illegal. Caught between the two legal systems, the airline industry insisted on the EU and the

---

[19] Ibid.

[20] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission report: Final report of the national commission on terrorist attacks upon the United States*, New York: W.W. Norton and Company, 2004, p. 385.

[21] See the Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108−458, 118 Stat. 3638, 17 December 2004, Section 4012(2).

[22] Council of the European Union, Directive 95/46/EC 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.

[23] The list of derogations is covered by Art. 26 of the Data Protection Directive.

[24] Indeed, only three countries and three British dependent territories have qualified according to the adequacy criteria of the European Commission: Jersey (2008), the Isle of Man (2004), Argentina (2003), Guernsey (2003), Canada (2002) and Switzerland (2000).

US finding a solution that would ensure legal certainty for air operators.[25] At the same time, the European Parliament and the Article 29 Working Party on Data Protection expressed various doubts about many aspects of a potential agreement, including its objective, the number of data items to be collected, the data retention period and the lack of means for extra-judicial appeal.[26] The broad implications for transatlantic trade and tourism made the European Commission adopt a more moderate approach.

In the joint declaration of February 2002, the European Commission and the US Customs and Border Protection expressed the opinion that all necessary measures should be taken "to reconcile and respect fully legal obligations on both sides leading towards a mutually satisfactory solution, providing legal certainty. For this purpose both sides [would] engage in an intense dialogue to reach a mutually satisfactory solution without delay."[27] The main challenge for the European Commission and the Council was to find a solution to legal problems posed by the US-based regulation. In the case of the PNR, the major issue was to provide legal certainty for the airlines operating transatlantic flights and to ensure that in the future similar regulations would be discussed well in advance. To facilitate these aims, both sides agreed to establish the High-Level Political Dialogue on Border and Transportation Security (PDBTS), for the discussion of various aspects of new policies. Eventually, the EU–US PNR deal was concluded in 2007 after the annulment of the 2004 Agreement by the European Court of Justice and the expiration of the Interim Agreement of 2006.[28]

2.2 The Commission's proposal for the EU PNR system

Several months after the conclusion of the EU–US PNR Agreement of 2007, the European Commission presented its proposal for a framework decision to establish the EU PNR system as a component of the EU's anti-terrorism package.[29] The introduction of this system was discussed in the Multidisciplinary Group on organised crime, with the most recent version of the proposal (incorporating the findings of Slovenian and French presidencies) being presented on 23 January 2009.[30] This initiative was puzzling given several European objections to a similar instrument as that implemented in the US. It is noteworthy that the rationale for the EU PNR system provided in the proposal is mostly internal[31] and includes no reference to the American PNR system or similar ones being established worldwide (only the references to ICAO[32] and

---

[25] P. Pawlak, "Transatlantic border and transport security cooperation: Can one swallow make a summer?", in D. Hansen and M. Ranstorp, *Cooperating against terrorism: EU-US relations post September 11*, National Defence College, Stockholm, 2007(b).

[26] European Parliament, Transmission of personal data by airlines in the case of transatlantic flights, European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: State of negotiations with the USA, P5_TA-PROV(2003)0429, 9 October 2003(b).

[27] European Commission, European Commission/US customs talks on PNR transmission: Joint statement, Brussels, 17-18 February 2003.

[28] For more details about these agreements, see E. Guild and E. Brouwer, *The political life of data: The ECJ decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July 2006; see also Argomaniz (2009), op. cit.

[29] European Commission, "Fight against terrorism: Stepping up Europe's capabilities to protect citizens against the threat of terrorism", IP/07/1649, Brussels, 6 November 2007.

[30] This proposal was the most recent at the time of writing. See Council of the European Union, Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/09, Brussels, 23 January 2009.

[31] The Hague Programme and the extraordinary Council meeting of 13 July 2005 are mentioned as two points at which the Commission was called upon to establish an EU PNR system.

[32] ICAO refers to the International Civil Aviation Organisation.

IATA[33] are made). Such an approach clearly suggests that the Commission is trying to avoid any association with the US PNR initiative in order to reduce internal opposition in the EU. The linkage between the EU and the US PNR systems would be more difficult to make if there were not a surprising similarity between the Commission's proposal and the provisions of the EU–US PNR Agreements (see Table 1).[34]

Table 1. Comparison of the EU–US PNR I, PNR III and the EU's PNR proposal

Issue	**EU–PNR PNR I**	**PNR III**	**EU PNR**
Purpose	Preventing and combating • terrorism and related crimes; • other serious crimes, including organised crime, that are transnational in nature; • flight from warrants or custody for the crimes described above.	Same as the PNR I; The PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law.	Preventing, detecting, investigating and prosecuting terrorist offences and serious crime; The EU PNR is applied solely to air transportation but member state authorities may expand it to other areas (Point 7a).
Sensitive data	The CBP will not use 'sensitive' data from the PNR. The CBP will implement an automated system that filters and deletes certain sensitive PNR codes and terms that the CBP has identified in consultation with the European Commission.	The DHS employs an automated system that filters sensitive PNR codes and terms and does not use this information. Unless the data is accessed for an exceptional case, the DHS promptly deletes the sensitive EU PNR data.	No risk-assessment criterion is to be based on sensitive data, although this does not exclude their collection; *but* the PIUs may exchange such data among themselves.
Data retention period	3.5 years – if the data have not been manually accessed during that period, they will be destroyed; 11.5 years – if accessed the data will be transferred to a deleted record file where they will remain for 8 years before they are destroyed.	15 years – after 7 years the data will be moved to a dormant, non-operational status; data in a dormant status will be retained for 8 years.	6-10 years – 3 years after their transfer and a further period of 3-7 years in archives; after that period, data should be deleted from the database.
Number of data items	34	34 (only 19 enumerated explicitly)	Same as in the PNR III

[33] IATA refers to the International Air Transport Association.

[34] Most of the differences can be explained with the complexity of EU decision-making procedures and the fact that various countries insisted on different provisions being inserted. Hence, for instance, the data retention period may vary from six to ten years.

Table 1. cont'd

Access to data by data subjects and redress mechanisms	Access – yes but it is conditional; Redress – the CBP will undertake to rectify data at the request of passengers and crewmembers, air carriers or data protection authorities in the EU member states (to the extent specifically authorised by the data subject), where the CBP determines that such data is contained in its database and a correction is justified and properly supported.	Access and redress – yes but it is conditional; The PNR III extended administrative protections under the Privacy Act to PNR data stored in the Automated Targeting System (ATS), regardless of the nationality or country of residence of the data subject.	Access – yes, but member states may adopt legislative measures restricting access to information; Rectification and erasure rights are provided but no organisation/body in particular is appointed as to deal with such requests; The data subject must have the right to seek judicial remedy for any breach.
Reciprocity of data transfers	No – the CBP shall, strictly on the basis of reciprocity, *encourage* US-based airlines *to cooperate.*	No – the DHS intends, strictly on the basis of reciprocity, to actively *promote the cooperation* of the airlines within the jurisdictions of the EU.	Yes – if specific conditions are met, including purpose, adequate level of data protection, etc.; in addition, in some instances there is no need for a decision on adequacy.

Source: Author's compilation based on Council of the European Union (2004), (2007a) and (2009).

Throughout the process of the EU–US PNR negotiations, major frictions arose with respect to the purpose of the agreement, the retention period, redress mechanisms and transfers of sensitive data.[35] The data retention period proposed in the Agreement (according to the US, at least seven to eight years) was problematic because, as argued by the Article 29 Working Party, it was "doubtful whether an excessively long data retention time with regard to millions of individuals can be effective for investigative purposes. …Data should only be retained for a short period that should not exceed some weeks or even months following the entry to the US. A period of 7-8 years cannot be considered as justified."[36] In addition, the list of 34 items of data to be collected was regarded as excessive, given that "no evidence or explanation has been provided about how their processing could be deemed to be necessary, proportionate and not excessive in a democratic society for combating terrorism".[37]

The European Commission initially subscribed to many of these criticisms but during the negotiations it softened its positions and proposed similar solutions to be introduced in the EU PNR system. Although the process and the content of the EU system differ from the American

[35] Sensitive data is that which may reveal race, ethnic origin or religious belief – the transfer of which is prohibited by the Directive 95/46/EC as a matter of principle.

[36] Article 29 Data Protection Working Party, Opinion 2/2004 on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, Brussels, WP 87, 29 January 2004.

[37] Ibid.

one, the result is still very similar to the final PNR Agreement negotiated with the US in 2007 (Table 1). In many instances, the scope of the EU provisions goes even farther than the EU–US PNR Agreement, which may suggest that the Commission used the momentum provided by the EU–US negotiations to advance its own controversial measures.[38]

The revised version of the proposal presented in January 2009 additionally includes provisions allowing member states "to provide, under their domestic law, for a system of collection and handling of PNR data for other purposes than those specified in this Framework decision".[39] The data collected by passenger information units (PIUs) in member states should be used to carry out "real time risk assessment of the passengers in order to identify the persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities of the Member State".[40] The PNR data will be processed against relevant databases and the risk criteria for the assessment will be provided under national laws. The problem is that each of the national PIUs will have the freedom to determine what constitutes a risk. The difference in risk assessment methods may form an obstacle to the freedom of movement in the EU. For instance, the same person may be prevented from boarding a flight to Belgium but be allowed on a flight to Germany. That is why Austria, Portugal, Slovakia and Luxembourg pleaded in favour of some degree of harmonisation with regard to the risk assessment.

Furthermore, Art. 8 of the EU PNR proposal stipulates that "PNR data and the analysis of PNR data may be transferred or made available by a member state to a third country only on a case-by-case basis" and only if certain conditions are met, including the necessity of such a transfer and an adequate level of protection for the intended data processing in that third country. In the case of onward transfers (i.e. when one member state wants to make available data received from another member state), the permission of the member state from which the data originates is required.

It is obvious, however, that 'the shadow of the future' will make authorities cooperate, i.e. they will be reluctant to refuse a request for information in case they might need similar data in the future. Even more worrying is the derogation from this principle provided in Art. 8.2, which stipulates that "data may be transferred to a third country without the prior consent of the Member State from which the data was obtained only if the transfer of the data is essential for the prevention of an immediate and serious threat". The question that remains is this: What does "immediate and serious threat" mean?

Other than content issues, the proceedings of the European Commission have resembled the American unilateral approach to the whole issue. One of the major criticisms raised by the EU with respect to the EU–US PNR was the lack of consultation or any discussion about the intentions of the US. Yet, while aware of the international implications of the system, the EU has not held discussions with its international partners.[41] Although intensive dialogue continues with developed countries such as the US, Canada and Australia, very little discussion is taking place between EU authorities and their counterparts in Eastern Europe or other countries where these instruments would apply.

---

[38] D. Bigo and S. Carrera, *From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU*, CEPS Commentary, CEPS, Brussels, 17 February 2007 (retrieved from http://ceps01.link.be/Article.php?article_id=314).

[39] Art. 7a, Council of the European Union (2009), op. cit.

[40] Ibid., Art. 3(3b).

[41] Derived from an interview with a European Commission official, DG RELEX, Brussels, February 2008.

3. How did we get here? Explaining the American influence

The objective of the US homeland security strategy is to detect, prevent and defeat any potential threats to American citizens.[42] To achieve it, the US approach focuses on ensuring that international security regulations provide for effective counterterrorism activities, and as deemed necessary, on improving regulatory standards in the territories of other countries.[43] This approach has further enhanced the US impact on transatlantic and EU security, mostly through its role as an agenda-setter and catalyst. At the same time, the increasing cooperation on homeland security has enhanced the role of some actors while sidelining others. The policy-making process has become dominated by informal networks and personal relationships, which have strengthened the mutual learning and trust-building dimensions of the EU–US homeland security cooperation. The following sections address these aspects in more detail.

3.1 The US as a catalyst and agenda-setter

The increasing focus on homeland security policies in the US has provided an impulse for the development and implementation of EU actions in this field. Many EU officials have confirmed that the post-9/11 developments in the US have had a spillover effect in Europe and created a window of opportunity for advancing security cooperation at the EU level. For instance, even though many policy proposals were presented in the Tampere conclusions, their implementation has progressed only since 2001. As one of the officials from the Directorate-General for External Relations (DG RELEX) put it, the EU was "unprepared" to work with the US mostly because the security consciousness did not develop as rapidly as it did in the US.[44] This also partly explains the big influence that the US has had on the transatlantic and EU security agendas.

A study of the progress achieved in the framework of the New Transatlantic Agenda and the Action Plan of 1995 demonstrates that the US was more effective in pursuing its own security objectives in the transatlantic context, and de facto shaped the EU policy agenda in this field.[45] From 2001 onwards, US efforts accelerated, coupled with increased engagement on the part of

---

[42] The White House, *National Strategy for Homeland Security*, Office for Homeland Security, Washington, D.C., July, 2002(b).

[43] Transnational regulation (as this practice is called in the academic literature) has its sources in the reciprocal interdependencies among actors (i.e. in areas of trade or security). More specifically, the focus on transnational regulation may stem from several concerns, including the achievement of a competitive advantage or to avoid a situation whereby such advantage is gained by the other side (K.W. Abbott and D. Snidal, "International 'standards' and international governance", *Journal of European Public Policy*, Vol. 8, No. 3, 2001; D. Lazer, "Regulatory interdependence and international governance", *Journal of European Public Policy*, Vol. 8, No. 3, 2001). It may also relate to gaining market access and economies of scale (K. Nicolaidis and M.P. Egan, "Transnational market governance and regional policy externality: Why recognize foreign standards?", *Journal of European Public Policy*, Vol. 8, No. 3, 2001) or accessing the information spreading through numerous informational networks (Lazer, 2001, op. cit.; M.L. Djelic, "Social networks and country-to-country transfer: Dense and weak ties in the diffusion of knowledge", *Socio-Economic Review,* Vol. 2, 2004; M.L. Djelic and K. Sahlin-Andersson (eds), *Transnational governance: Institutional dynamics of regulation*, Cambridge: Cambridge University Press, 2007). In the case of international homeland security, the major reason for the development of transnational regulation has been to avoid regulatory imbalances and the emergence of 'safe heavens', which would mean increased insecurity for all parties.

[44] Derived from an interview with a European Commission official, DG RELEX, Brussels, March 2009.

[45] J. Peterson, H. Wallace, M.A. Pollack, R. Doherty, F. Burwell, J.P. Quinlan and A. Young, *Review of the framework for relations between the European Union and the United States: An independent study*, European Commission, Brussels, 2005.

the EU. Still, looking at the issues put on the agenda by EU representatives (i.e. data protection, visas and biometric identifiers), the reactive nature of their approach is noticeable. In most cases where the EU has shown interest, it has been dictated by the need to respond to American legislation. This argument coincides with that presented by Statewatch in its bulletin of 2007, where authors argue that "the 'US/EU channel' is largely a 'one-way street' for US demands. It is rarely used by the EU to meet its needs and when it does it faces intransigency."[46] Therefore, it can be argued that the US has contributed to raising awareness in the EU of several security issues that were earlier beyond the EU agenda.

The US officials are convinced that for the EU, it has also been the occasion to prove itself and improve its international standing. As suggested by one of the US officials in the Department of State, "one should not underestimate the attention that the EU wants to get from the US".[47] For that reason, when presiding over the European Council, Prime Minister Guy Verhofstadt asked the American representatives to suggest issues on which both sides could enhance cooperation against terrorism. Since "nobody wanted to prepare this list", it was eventually drafted in Washington and sent for dissemination in Brussels. The list prepared for the Commission President Romano Prodi was leaked to the media and publicised as the "49 American demands".[48] Presented in the EU as "a sweeping agenda covering unregulated and unaccountable powers affecting criminal investigations, suspects' rights, the retention of telecommunications data, border controls and asylum policies", this letter created many problems. In the aftermath, the US had to organise several separate meetings because "people from [the] first and third pillar[s] did not want to sit in the same room".[49] Although this situation has had a limited impact on EU–US cooperation, it has clearly demonstrated that American involvement in EU security policies remains a sensitive topic and almost taboo.

3.2 New actors and informal networks

The bilateral cooperation between the EU and the US has developed in the framework of the New Transatlantic Agenda of 1995, which – through the process of summits, senior-level group meetings, task forces and civil society dialogues – has been expected to provide a suitable environment for the advancement of transatlantic relations. Initially, membership in these bodies was mostly limited to diplomats and trade specialists from both sides, with the ad hoc presence of specialists on other topics if the agenda of a meeting so required.

The growing external exposure of once internally-oriented agencies and services (i.e. in the US these were Customs and Border Protection and the Department of Justice) resulted in the emergence of new actors and their constellations. Currently, the issues related to the fight against terrorism are dispersed across the EU among several institutions and directorates-general in the European Commission, including the DG for Justice, Freedom and Security (DG JFS), the DG for Transportation and Energy (TREN), the DG for Taxation and Customs Union (TAXUD) and DG RELEX.[50] Although some of them have acted at the international level in the

---

[46] Statewatch, "EU/US security 'channel' – A one-way street?", *Statewatch Bulletin*, Vol. 17, No. 1, 2007 (retrieved from www.statewatch.eu).

[47] Derived from an interview with a former US official, Department of State, Washington, D.C., May 2007.

[48] The text of this letter is available on the Statewatch website (http://www.statewatch.org).

[49] Derived from an interview with a former US official, Department of State, Washington, D.C., May. See also the Statewatch website article at http://www.statewatch.org/news/2001/nov/06Ausalet.htm.

[50] The focus here is mostly on the European Commission, which assumed the leading role in the field of homeland security and by its nature is supposed to represent Community interests. Yet, the network of EU security actors is more extensive and complicated. See for instance, CERI/Sciences Po-CNRS

past (DG TAXUD and DG TREN), the scope of their activities has been rather limited. Similarly, the DG JFS has developed its international expertise in the context of previous enlargements, but it has mostly been the fight against terrorism that has put it in the spotlight and contributed to the most dynamic growth of its external activities.[51] Gradually, a small task force that had been established to prepare third countries for EU membership became an extensive policy unit.[52] Nowadays, all directorates-general involved in various aspects of internal security issues have units dealing explicitly with external relations and individual officers responsible solely for contacts with the US (which used to be the domain of the DG RELEX).

In time, the predominantly diplomatic representation in the meetings began to provoke unease among the homeland security professionals – dubbed 'securocrats' by this author – who questioned the qualifications of trained diplomats in areas of law enforcement, counterterrorism, etc.[53] As the agenda increasingly included homeland security issues, these fora became overcrowded and ineffective.[54] Their formality and structure of membership led the securocrats to establish their own specialised and more informal bodies,[55] with the objective of ensuring that those doing conceptual thinking on either side actually talked to one another.[56] The emergence of networks with more organisational and cultural homogeneity[57] between EU and American officials provided a new dynamism at the transatlantic level and proceeded simultaneously to engender more inter-organisational rivalries and conflicts.

CHALLENGE Research Group, "Mapping of the European Security Agencies", CERI/Sciences Po-CNRS, Paris, 2008 (retrieved from www.libertysecurity.org/article1670.html).

[51] According to a former EU official from the DG JFS, initially the unit was mostly engaged in the enlargement negotiations and prepared the Commission's position on issues of justice and home affairs. Gradually, many issues resolved during the enlargement process (although not explicitly covered by the *acquis communautaire*) became the subject of cooperation with third countries, i.e. capacity building of the judiciary, police cooperation and border control. Consequently, the European Council at Feira in 2000 asked the European Commission to present a communication on the external dimension of EU justice and home affairs (derived from an interview with a European Commission official, DG RELEX, Brussels, March 2007).

[52] For more on the development of the external dimension of justice and home affairs policies, see P. Pawlak, "The External Dimension of Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization?", *Journal of European Integration*, Vol. 31, No. 1, 2009(a), pp. 25-44; see also S. Alegre, *The EU's External Cooperation in Criminal Justice and Counter-terrorism: An Assessment of the Human Rights Implications with a Particular Focus on Cooperation with Canada*, CEPS Special Report, CEPS, Brussels, September 2008.

[53] One of them raised a rhetorical question: "Do diplomats understand anything about security?" Derived from an interview with a European Commission official, EU Delegation, Washington, D.C., February 2007.

[54] P. Pawlak, "From Hierarchy to Networks: Transatlantic Governance of Homeland Security", *Journal of Global Change and Governance*, Vol. 1, No. 1, 2007(a).

[55] It is noteworthy that the US is the only major partner of the EU with whom there is no overlapping legal framework to regulate the relationship. Both the New Transatlantic Agenda and the most recent developments are taking place based on political declarations, with the exception of sectoral EU–US international agreements. Still, bodies like task forces or high-level dialogues exist and have a limited basis in the EU Treaties.

[56] See Pawlak (2007a).

[57] For more on the issue of homogeneity in transatlantic networks, see P. Pawlak, "Network politics and transatlantic homeland security cooperation", *Perspectives on European Politics and Society*, Vol. 10, No. 4, Special Issue, 2009(b), forthcoming in December.

In 2004, the EU and US agreed to create the above-mentioned PDBTS. It was intended as an early warning mechanism, to facilitate discussion of controversial legislation before it provoked conflict. The initiative came from the homeland security professionals, who – constrained by the existing diplomatic channels – felt the need to move their cooperation beyond the platforms of diplomatic 'talking shops' and instead focus more on results.[58] Since the PDBTS was created outside the formal EU institutional framework,[59] it was able to develop flexibility in terms of its format, membership and functioning. Moreover, because it did not constitute part of a formal negotiation process but rather a forum for exchange of information, the PDBTS allowed for more frank discussions. As Jonathan Faull, director-general of the DG JFS, said during a press conference after the first meeting of the PDBTS, its participants have "deliberately decided to avoid the usual pleasantries and long speeches and reading of documents which everybody should have read, no doubt, has read anyway. But we got down to brass tacks very quickly. These are issues of the greatest importance for the security of citizens of the European Union and of the United States."[60] Several rounds of PDBTS meetings have proven a good opportunity for EU and American policy-makers not only to resolve persistent problems, but also to learn more about each other and exchange information, and they have consequently contributed to building trust and relationships.[61]

3.3 Learning and building trust

Since the transfer of data to the US authorities represented a breach of EU data protection laws, the only option for the European Commission was to establish whether the US data protection system was 'adequate' by EU standards and only then give the green light to the airlines. This task was difficult not only owing to differences between the EU and American approaches to data protection, but also to the entire transatlantic context (i.e. the wars in Iraq and Afghanistan, and the controversies over Guantanamo and extraordinary renditions).

One of the problems that emerged at the transatlantic level in the post-9/11 context was the limited trust between policy-makers on both sides and the role of emotions in the process. When asked about the most challenging aspects of transatlantic security cooperation, one of the EU officials suggested that "people's reciprocal fears, interests and emotions are important and need to be taken into account. They definitely do not make things easier. …Homeland security is more than business and profits. That is why it is more challenging."[62] Initially, the presence of new actors at the transatlantic level proved difficult – mostly because it was the first time many of them had met.[63] Nevertheless, the cultural and organisational proximity among some

---

[58] Ibid.

[59] 'Formal' in this sense means based on treaties or other interinstitutional arrangements.

[60] The US Mission to the European Union (2004), *US, EU discuss transportation, border security*, Brussels, 27 April (retrieved from http://useu.usmission.gov/Article.asp?ID=3B93FC1F-F30E-467D-A287-54777BE14CE7).

[61] Derived from interviews with EU and US officials, October 2006–July 2007.

[62] Derived from an interview with a European Commission official, DG External Relations, Brussels, October 2006. Similar views prevailed among officials interviewed for the purpose of this research. For instance, another person described the problem in the following way: "Because we are dealing with the US, a lot of debates are rather embedded in a broader political context and therefore become very emotional. The subject as such is already important but [the] emotions involved make the whole issue even more difficult."

[63] One of the US officials referring to his first experiences with the EU had this comment: "First, it was [an] educational problem. I came from the Congress and there we were not worried about the EU at all. So we had to learn that the EU can actually be a useful partner and not be seen only as a necessity."

individuals very soon led to the emergence of new coalitions, most notably of internal security officials. The progressive emergence of trust and relationships among them has allowed the cooperation to move beyond the formality of international law instruments.

The issue was complicated because from the beginning the data protection authorities in member states and the European Parliament took a very strict stand on the US requirements. In one of its early opinions (2002), the Article 29 Working Party expressed the view that "it does not seem acceptable that a unilateral decision taken by a third country for reasons of its own public interest should lead to the routine and wholesale transfer of data protected under the directive".[64] In the same opinion, it was argued that because the data forwarded by airlines related to identifiable physical persons and was processed by airlines within the EU, they were protected by the provisions of the Data Protection Directive (95/46/EC). Therefore, access to passenger data violated the EC Regulation on computer reservation systems as well as the 1995 Data Protection Directive.[65] Criticism was also expressed of the purpose and proportionality of the measures adopted. While data protection authorities recognised the need to combat terrorism, they also underlined that "the respect for fundamental rights and freedoms of the individuals including the right to privacy and data protection must be ensured".[66] In June 2003, the Article 29 Working Party reiterated that "the legitimate requirements of internal security in the United States of America may not interfere with these fundamental principles".[67]

A similar position was taken in resolutions and reports of the European Parliament. The European Parliament resolution of 2003 raised a number of issues that in their opinion were not satisfactorily resolved and therefore needed further discussion. The European Parliament presented several objections: the scope of the agreement was unclear, the request for access to 39 data items seemed "excessive and under all circumstances out of proportion" and the data retention period of six or seven years was "unjustified", especially in the cases of those persons who "do not present any risk to the country's security".[68] Aware of the implications of the negotiated deal, in its resolution of 2004 the European Parliament stated that it was "extremely important that the outcome of the negotiations [was] not [to] be taken as a model for the EU's further work on the development of its own anti-crime measures, data storage and protection of confidentiality".[69]

Derived from an interview with a former US official of the Department of Homeland Security, Washington, D.C., May 2007.

[64] Article 29 Data Protection Working Party, Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States, 11647/02/EN, WP 66, Brussels, 24 October 2002.

[65] Ibid.

[66] This stems not only form the Directive but also from the Art. 8 of the European Convention on Human Rights and Arts. 7 and 8 of the Charter of Fundamental Rights of the European Union. See Article 29 Data Protection Working Party, *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism,* 0901/02/EN/Final, WP 53, 14 December 2001.

[67] Article 29 Data Protection Working Party, Opinion 4/2003 on the level of protection ensured in the US for the transfer of passengers' data, 11070/03/EN, WP 78, Brussels, 13 June 2003.

[68] European Parliament, Resolution on transfer of personal data by airlines in the case of transatlantic flights: State of negotiations with the USA, P5_TA-PROV(2003)0429, 8 October 2003(a).

[69] European Parliament, Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, 2004/2011(INI), P5_TA-PROV(2004)0245, 2004.

In light of such extensive opposition, the adequacy decision of the European Commission[70] with respect to the US was a surprising move. Given that the US Customs and Border Protection was asked to provide additional safeguards, a conclusion can be reached that the decision establishing the adequacy of the American data protection system was politically motivated rather than based on an objective assessment. Even more interesting is the evolution of this 'quasi-legal' instrument from the Undertakings in 2004[71] and the letter to the Council presidency and the Commission from the DHS in 2006,[72] to the US letter to the EU accompanying the PNR Agreement of 2007.[73]

The outcome of the 2004 negotiations was puzzling because it was a hybrid composed of a rather loose international agreement and very detailed Undertakings, presented in the form of a political commitment rather than a legally binding document. Bearing in mind that the most contentious provisions of the entire package were incorporated in the Undertakings (i.e. the use of PNR data, data requirements, storage and methods of accessing the data), it was surprising that the EU agreed to such a weak form. According to its text, the Undertakings make up a unilateral declaration of the US Customs and Border Protection to follow certain principles and rules with regard to the treatment of PNR data. Thus, the Undertakings constitute a complementary act with the objective of providing additional guarantees for the EU. The outcome, although slightly uncomfortable for lawyers and unsatisfactory from an international law perspective, was considered a necessity from the political perspective.[74]

During the PNR negotiations in 2006 and 2007, similar provisions to those in the Undertakings were included in the format of letters 'from the US to the EU'. Since the legal basis for the agreement transferred from the first pillar to the third pillar (i.e. which is beyond the scope of the EU Data Protection Directive and hence not subject to the 'adequacy finding' procedure), this exchange of letters was meant to serve as a commitment of both sides to respect one another's data protection regime. The following except is drawn from a reply from the EU to the US:

> While taking note of the content of your letter, we wish to reaffirm the importance that the EU and its Member States attach to respect for fundamental rights, in particular to the protection of personal data. The commitments of DHS to continue to implement the Undertakings allow the EU to deem that, for purposes of the implementation of the Agreement, it ensures an adequate level of data protection.[75]

This reliance upon soft modes of regulation rather than on formal legal arrangements is an interesting and important development. It demonstrates that informal contracts have increasingly compensated or substituted the formal contractual safeguards, which in the light of

---

[70] European Commission, Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235, Brussels, 06.07.2004.

[71] Department of Homeland Security, Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), DHS, Washington, D.C., 11 May 2004(a).

[72] Council of the European Union, Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the Undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of Passenger Name Record (PNR) data, 13738/06, Brussels, 11 October 2006.

[73] Council of the European Union (2007a), op. cit.

[74] Derived from an interview with a US official, Department of State, Washington, D.C., May 2007.

[75] Council of the European Union, Reply by the Council Presidency and the Commission to the letter from the USA's Department of Homeland Security, 13835/06, Brussels, 13 October 2006.

empirical evidence can be interpreted as a sign of learning and increasing trust among the parties. For instance, when commenting on the PDBTS, Jonathan Faull had the following observation:

> There is no doubt that we share one hundred percent the same objectives in making our borders secure, making our transport systems secure and in striking the right balance between the security measures and the rights of the individual and the protection of data. Those are our objectives. I think they are absolutely common. We have different legal systems, different political structures, so the way[s] we get there are not always the same. But the more we talk to each other, the more likely it is that we will find common paths to that common destination.[76]

Similarly, Tom Ridge, former US secretary for Homeland Security, reflected on these developments in the following way:

> What I have discovered is that when we sit down, make our case, discuss, negotiate finding a common solution of mutual benefit, we've made a lot of progress. Part of me wishes we'd started that a little bit earlier, but there were other things that it seemed at the time were higher priorities.[77]

Some officials also believe that "those [at] the top are having better contacts between themselves and are more open to pragmatic discussion",[78] which has helped to transform the American "bunker mentality"[79] into a more open one.

3.4 The development of personal relationships

The role of this dialogue and the personal relationships established between officials on both sides of the Atlantic cannot be underestimated. Personal relations "make a really great deal" and help to "push things forward".[80] Their role has been acknowledged at the highest political levels.[81] Personal and informal relationships that developed between the EU and American officials through participation in the same fora created an environment for more informal discussion about transatlantic data exchange and data protection. Dialogues and interpersonal relationships have also had an impact on building a common understanding and empathy among officials involved in the process. This was needed because initially each side found it "[difficult] to see and understand" the other's perspective.[82] Since "privacy is not easy to understand", dialogues such as those of the PDBTS gave the policy-makers "time to work through concepts",

---

[76] US Mission to the European Union (2004), op. cit.

[77] Department of Homeland Security, Transcript of Secretary of Homeland Security Tom Ridge, DHS, Washington, D.C., 30 November 2004(b) (retrieved from http://www.dhs.gov/xnews/releases/press_release_0562.shtm).

[78] Derived from an interview with a European Commission official, DG Transport and Energy, Brussels, March 2007.

[79] Ibid.

[80] Derived from an interview with a Council Secretariat official, Brussels, March 2007. For an example of how individuals and broken relationships may have a negative impact on socialisation and the relationship at large, see Pawlak (2007b), op. cit. One of the officials, for instance, mentioned that "the attitude" towards Europeans was expressed, among others, in conducting negotiations in very limited spaces and "terrible" conditions.

[81] Derived from an interview with a European Commission official, DG External Relations, Brussels, October 2006.

[82] Derived from an interview with a former privacy officer, Department of Homeland Security, Washington, D.C., March 2007.

along with a chance to clarify "differences in language" and "to listen to each other more and get a better understanding".[83]

Similar objectives were behind the creation of the High-Level Contact Group (HLCG) on data protection. Established by the decision of the EU–US Justice and Home Affairs Ministerial Troika on 6 November 2006, the HLCG started its work as an informal advisory group bringing together EU and US policy-makers (i.e. senior officials from the Commission, the Council presidency supported by the Council Secretariat and the US Departments of Justice, Homeland Security and State). The DG JFS, represented by both security and data protection specialists, was the leading actor on the EU side.

The HLCG was intended to provide broader reflection on the methods that would allow for effective law enforcement cooperation while at the same time ensure a high level of data protection. It was an opportunity for EU and American policy-makers to enhance their mutual understanding of working methods, progress towards "common principles" and eventually establish "an effective regime for privacy and personal data protection".[84] A set of core privacy and personal data protection principles was identified during the first meeting of the group on 26 February 2007, and another informal expert group was set up with the aim of developing agreed definitions of those principles.[85] Operationally, the expert group and the HLCG relied mostly on videoconferences and electronic transfers of documents. Draft documents were exchanged between the two sides ahead of videoconferences and then thoroughly discussed. Political leaders endorsed the final report of the HLCG at the EU–US summit in 2008.

The history of the HLCG would be incomplete without mentioning the role that individuals and personal relationships between EU and US officials played in the creation of this group. The HLCG emerged from the PDBTS as a new, even more specialised body. The idea came from a former official at the US Department of Justice based in Brussels, Mark Richard, and was implemented thanks to his close relationship with Gilles de Kerchove at the Council Secretariat. They were both involved in the negotiations of the PNR agreements and in the SWIFT talks. They also both agreed that many problems during the process emerged from a limited knowledge of one another's data protection systems rather than from differences between them.[86] Therefore, the new informal group was "an attempt to take privacy out of the negotiation context and try to look at issues objectively".[87] This forum, bringing together data protection specialists from both sides of the Atlantic, operates beyond any formal institutional mandate and relies fully on informal contracts among its members.

The emergence of personal relationships among officials led to two other noteworthy developments at the transatlantic level. First, the traditional dividing line between the EU on one side and the US on the other side has faded and given rise to a more complex set of functional dichotomies between the legislative and executive branches or between diplomats and security professionals. The differences of approach and objectives of these groups have sometimes fostered a new dynamic in transatlantic relations, as in the case of the EU–US PNR Agreement.

---

[83] Derived from an interview with a US official, Department of Homeland Security, Washington, D.C., April 2007.

[84] Council of the European Union, *Final Report by EU-US High-Level Contact Group on information sharing and privacy and personal data protection,* 9831/08, Brussels, 28 May 2008(b).

[85] Ibid.

[86] Derived from an interview with a US official, Department of Justice, Washington, D.C., February 2009.

[87] Derived from an interview with a US privacy officer, Department of Justice, Washington, D.C., April 2007.

More importantly, the emergence of the PDBTS as a new body in the EU–US policy-making architecture and the resulting shift from a formal negotiation context to a more informal and less transparent environment has strengthened the objections of those stakeholders who were denied access to the process. The outcomes stemming from the conflicts surrounding the process have eventually affected the final policy, which in the case of the EU–US PNR Agreement moved the agreement from the Community's first pillar (as was the case of the PNR I Agreement) to the third pillar (as is the case of the PNR III Agreement).[88]

Personal ties between policy-makers on both sides of the Atlantic have also contributed to the surfacing of issue-based transatlantic coalitions, in which each side has supported the other in their domestic struggles. For instance, EU officials have talked with the US Congress and presented arguments in support of the position taken by the DHS,[89] while the DHS has talked with member states and the European Parliament and presented arguments in support of the stance taken by the Commission or Council. Second, personal relationships between the EU and US officials have had an impact on the evolution of particular legal and policy instruments. The reliance on soft regulation with flexible interpretation and a 'quasi-legal' framing of matters of great importance and sensitivity, such as the exchange of personal data, undoubtedly represents an interesting development.

4. What future for the EU data protection regime?

The progressive reliance on personal data and the exchange of such data for law enforcement purposes poses several challenges for global data protection and security. The transposition of existing data protection rules that were primarily set up for commercial purposes into a new, security-oriented policy context has proven particularly difficult. The discussion in previous sections reveals several elements that have important implications for the future of the EU data protection regime and the role of the EU in setting global data-protection rules. Numerous questions persist about the legal and political construction of the EU data protection system and its potential evolution, the role of stakeholders in the policy-making process, and finally the transparency and legitimacy of the process itself.

4.1 Legal issues

The conclusions reached by the HLCG read that the EU and US concur on an international agreement on data exchange as a preferred option for regulating transatlantic cooperation in this field.[90] In view of the US preference for soft laws and flexibility as expressed during earlier negotiations, this outcome is unexpected unless one takes into account a more general context

---

[88] For a more extensive discussion, see Pawlak (2009a).

[89] A very good example in this respect is the debate about the H.R. 1 Act (Implementing the 9/11 Commission Recommendations Act of 2007) assuming 100% screening of containers.

[90] The report of the HLCG and the summit conclusions of May 2008 were further endorsed in December 2008 in a special political declaration issued by EU and US officials:

> In order to ensure the continuation of law enforcement exchanges and practices between the United States and the European Union, both sides state that they are guided by the principles described above, on which consensus has been reached, until such time as a binding international agreement is concluded and without prejudice to outstanding issues to be further explored in that context.

Still, the statement included in the conclusions of the HLCG leaves the outcome open. See Department of Homeland Security (DHS), Statement on Information Sharing and Privacy and Personal Data Protection between the European Union and the United States of America, DHS, Washington, D.C., 12 December 2008(b) (retrieved from http://www.dhs.gov/xabout/international/gc_1229359375601.shtm#0).

and accepts that "there are ways to write things that mask the ambiguity".[91] While the US may still prefer soft regulation, which allows for more flexibility, the developments in the EU and uncertainties that they create complicate the discussion and prolong the entire process. Two issues are particularly significant: the application of the adequacy principle in the Framework Decision on data protection in the third pillar and the provision of an effective mechanism for judicial redress.

One of the reasons the US advocated an international agreement was adoption by the EU of the Framework Decision on the protection of personal data.[92] The Framework Decision applies to cross-border exchanges of personal data in the context of police and judicial cooperation. The rules for the transfer of data to third countries and international bodies rely on the same principle of adequacy as that of the EU Data Protection Directive of 1995. This means that such transfers are allowed if "the third State or international body concerned ensures an adequate level of protection for the intended data processing".[93] The determination of adequacy requires a decision by each member state that allows the EU states to negotiate a higher level of safeguards for protecting personal data than those established in the Framework Directive. That would subject the US to discussions with 27 countries with different data protection laws. The American side wanted to avoid any potential delays caused by the discussion about the adequacy of the US data protection system (as had occurred with the EU–US PNR Agreement), and hence they proposed the conclusion of an international agreement.

The adequacy principle included in that document and the impact of the Directive on global data sharing remain very problematic for the US, which describes it as an "ineffective and unworkable policy" that might cause a "potential disaster for the global war on terror".[94] The opposition of the US to the EU's principle of adequacy questions the EU approach to data protection and undermines it internationally. As observed by the Deputy Assistant Secretary for Policy at the Department of Homeland Security, Paul Rosenzweig, "the EU should reconsider its decision to apply notions of adequacy to the critical area of law enforcement and public safety. Otherwise, the EU runs the very real risk of turning itself into a self-imposed island, isolated from the very allies it needs."[95]

Another issue that remains unresolved is the question of judicial redress. The construction of the American data protection system (through the Privacy Act of 1974) does not provide for foreigners to initiate a judicial procedure in US courts. This situation can be remedied only through a change in the US law, which is a sole competence of the US Congress. For that to take place, the impulse would need to come from a very high political level, but there few chances of this happening. A study prepared by the General Accountability Office (the investigative body of the US Congress) in 2008

---

[91] Derived from an interview with a US official, Department of State, Washington D.C., February 2009.

[92] The Decision was adopted by the Council and published in the *Official Journal* on 30 December 2008 with the implementation deadline set for 27 November 2010. See Council of the European Union, Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008(a).

[93] See Art. 13(1d). Art. 14 provides a further explanation of how adequacy will be assessed:

> The adequacy of the level of protection referred to in paragraph 1(d) shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply.

[94] P. Rosenzweig, "Seven questions for the European Union", *Privacy & Security Law Report*, Vol. 6, No. 46, 2007.

[95] Ibid.

outlined several proposals for how to update the Privacy Act but none of them included the possibility of access to US courts by non-Americans. Still, to address the EU's concerns, the US proposed establishing an administrative process that would constitute an effective redress mechanism for EU citizens. This option was rejected by the EU side, which insists on 'judicial' rather than 'effective' redress.

The direction taken by the EU and US departs from a general practice of mutual recognition of agreements. This is because of the EU concept of an 'adequacy finding', which makes the process more unilateral than reciprocal (i.e. the EU determines the adequacy of another data protection system rather than both sides recognising one another's systems). This concept is controversial in the US for several reasons and increasingly faces opposition. More and more, American policy-makers are raising the following question: Is the EU data protection system adequate with respect to ours? Therefore, any future EU–US agreement will most probably bear some resemblance to a mutual recognition agreement to ensure that the process is reciprocal.

4.2 Governance issues

The participation of the legislative branch in the debate seems primarily to be an EU problem. The US political system gives the executive clear competence in the field of foreign policy, which is not always the case in the EU. The ambiguity of the EU decision-making procedures and a blurring divide between the internal and external aspects of policies make the process complicated. These characteristics have ramifications on the transatlantic partnership, as was evident in EU–US PNR Agreement. The role of the European Parliament also remained ambiguous with respect to the HLCG. While members of the European Parliament did not participate in the meetings, it was the understanding of the US side that the European Commission would "make sure that things on their side were working",[96] including communication with the European Parliament and other stakeholders. But that did not prevent the European Parliament, data protection authorities or the Article 29 Working Party from seeking information directly from the US – a situation that was both "uncomfortable" and "ironic" from the US perspective.[97]

The future role of the European Parliament was unclear until recently, owing to the pending adoption of the Lisbon Treaty, which had further connotations for the Commission's negotiation mandate. But the ratification of the Treaty by the Czech Republic brings slightly more certitude. Still, the new Treaty cuts both ways for the US. The biggest "advantage"[98] in the current institutional and legal environment is the limited role of the European Parliament. The adoption of the Lisbon Treaty, while simplifying the EU decision-making process, creates a new legal context. The pillar structure will disappear and the role of the European Parliament will increase.[99] In addition, the change of the European Commission and the European Parliament in the course of 2009 will cost the entire process more time.

Furthermore, although the focus of this paper is on the political dialogue on border security and data protection in the transatlantic context, one needs to keep in mind that this is only part of the picture. Similar networks have been established among officials dealing with customs security

---

[96] Derived from an interview with a US official, Department of Homeland Security, Washington D.C., February 2009.

[97] Ibid.

[98] Ibid.

[99] This is one of the reasons the European Commission has recently decided to accelerate discussions with the US regarding the conclusion of a new deal on the SWIFT data transfers. See J. Crosbie, "Commission to seek new deal with the US on data transfers", *European Voice*, 16 July 2009.

(the Joint Customs Cooperation Council) and transportation security (the Transportation Security Cooperation Group). The idea behind the latter group is mostly to inform one another in advance about planned initiatives and to take actions jointly. Consequently, the EU and US officials visit airports on both sides of the Atlantic to learn how each side operates and eventually to foster mutual trust and recognition of standards.[100] In addition, there are several other more informal networks between Europol and FBI officials, between the US Customs and Border Protection and EU FRONTEX staff, and among law enforcement officers at operational levels.

Considering the sensibility of the issues, the emergence of such informal channels is not surprising. Intelligence cooperation among countries is essentially based on such initiatives. But what does it mean for the policy-making process? As already indicated, most of these networks only include representatives of the executive with very limited access accorded to legislative and data protection bodies. The most recent developments in the EU–US cooperation on data exchange confirm the general trends identified in this paper. First, we observe the proliferation of informal networks between American and EU policy-makers. These networks operate beyond any legal mandate provided in the Treaties and their operations are based on informal relationships among individuals. This is best expressed in the introduction by the Czech presidency to the HLCG final report: "The Presidency would like to highlight that this draft final report as such is not a report by the Council or by the EU, but by the High-Level Contact Group." If the HLCG does not represent the Council or the EU, for whom does it speak? And what is the significance of its conclusions?

The implications of these networks for the EU's security policies cannot be underestimated. While the potential effects of transnational regulation are rather straightforward and can be identified rather easily, the processes of building trust and learning in these networks are much more difficult to observe. Therefore, they require more careful investigation. On the one hand, they provide the opportunity for the exchange of information and learning, which makes any discussion "more fair intellectually".[101] On the other hand, they affect the EU's internal organisation, its working methods and approaches to policies,[102] and hence need to be scrutinised.

5. Policy recommendations

As this paper has demonstrated, informal policy-making at the transatlantic level is playing an ever-larger role. This can be interpreted as a sign of the integration process progressing outside any official framework. Yet, this process suffers from a lack of transparency and dubious legitimacy. While it is understandable that some issues need to be discussed behind closed doors, the level of secrecy and the number of obstacles to obtaining any related information are difficult to justify. It is possible that, as policy-makers claim, the informality and flexibility of transatlantic networks allow for working towards more innovative and possibly more efficient solutions. But because of the extensive scope of homeland security policies and their repercussions for individuals, the information provided to the public should be more detailed rather than fragmented and imprecise.

---

[100] Derived from an interview with a European Commission official, DG Transport and Energy, Brussels, 14 March 2007.

[101] Derived from an interview with a former US official, Department of Homeland Security, Washington, D.C., April 2007.

[102] For a discussion of the impact of the internal EU debate about the EU–US PNR Agreement on the balance and the context of EU counterterrorism policies, see Pawlak (2009b).

The above considerations raise several critical issues that should be addressed in light of the discussions underway about the Stockholm Programme. In its Communication to the European Parliament and to the Council, the Commission suggests that "[t]he Union must respond to the challenge posed by the increasing exchange of personal data and the need for utmost respect for the protection of privacy… A comprehensive protection scheme should be introduced."[103] The following sections offer a number of recommendations that might be useful in future discussions about the implementation of this objective. The focus is on four elements in particular: the place of the citizen in the policy, the transparency and accountability of the process, the involvement of crucial stakeholders, and issues of global – including transatlantic – governance of data protection.[104]

5.1 Putting the citizen back in the centre of the debate

Whereas policy-makers see many benefits in the informality of networks and their potential to expedite the entire process, there is no doubt that from the perspective of an individual, this approach is problematic. The major problem is that the liberty and security of individuals are subjected to informal networking processes over which they have no control. Therefore, any future endeavours to strengthen the external dimension of security policies (i.e. within the Stockholm Programme) should also enhance the provisions about guarantees of fundamental rights and civil liberties.[105] Given the prevalence of the security mindset in the European Commission and in the Council, this objective could be achieved by giving broader access to policy-making to those actors specifically tasked with the protection of civil liberties and data protection, including the Fundamental Rights Agency and European Data Protection Supervisor.

In reference to the US, the EU should not only 'import' policies aimed at improving security, but also those that strengthen liberty and justice. While the EU is convinced of the supremacy of its data protection system,[106] many aspects of the US approach to data protection could be beneficial to EU citizens.[107] Two instruments that could be introduced to the EU decision cycles are the privacy impact assessments (PIAs) and the System of Record Notices (SORNs). The objective of the PIAs is to demonstrate that owners and developers of a specific programme or system "consciously incorporate privacy protections throughout the entire system development lifecycle".[108] SORNs, on the other hand, are required for systems operating with personal data.

---

[103] European Commission (2009), op. cit., p. 8.

[104] For a more extensive set of recommendations for a broader Area of Freedom, Security and Justice, see E. Guild, S. Carrera and A. Faure-Atger (2009), *Challenges and prospects for the EU's Area of Freedom, Security and Justice: Recommendations to the European Commission for the Stockholm Programme*, CEPS Working Paper No. 313, CEPS, Brussels, April 2009; see also E. Guild and S. Carrera, *Towards the next phase of the EU's Area of Freedom, Security and Justice: The European Commission's proposals for the Stockholm Programme*, CEPS Policy Brief No. 196, CEPS, Brussels, 20 August 2009.

[105] See also the policy recommendations in Guild, Carrera and Faure-Atger (2009), op. cit.

[106] Such a conclusion has been reached after numerous interviews with EU officials. Also, some official expert reports prepared by the European Parliament sustain this position. See European Parliament (2008), op. cit.

[107] For more information about the US data protection system (not only legal acts but also and most importantly mechanisms implemented in the process of policy-making), see Department of Homeland Security (DHS), *Department of Homeland Security Privacy Office Annual Reports to the Congress available* (retrieved from http://www.dhs.gov/xinfoshare/publications/editorial_0514.shtm#1).

[108] According to the PIA guidance, the impact assessments should include such elements as the scope of the information collected, uses, information security and information sharing. Furthermore, each section should conclude with an analysis outlining any privacy risks and discuss any strategies or practices used

They describe the purpose of the collection, the degree of information sharing, the categories of records and individuals covered, record retention and destruction, and how the records are retrieved within the system.[109] The introduction of such measures to the EU system, implemented simultaneously with a stronger role for national data protection authorities, the Article 29 Working Party and the EU Data Protection Supervisor, could improve the legitimacy of the process and render some controversial policy measures more acceptable to the public.

5.2 More transparency and accountability

The above analysis also raises many questions about the allegiances of major EU actors. As correctly noted by some of the observers, the positions of the European Commission and the Council seem to give more consideration to US national interests than they do to representing those of EU citizens. Therefore, there is a clear need for improvements to the transparency and accountability of the process, which may contribute to diminishing suspicion among the public. This can be achieved in several ways.

Parliamentary oversight needs to be improved. The abolition of the pillar structure through the Treaty of Lisbon is a good step in this direction since it gives the European Parliament a larger role under the co-decision procedure. Nevertheless, even the formal procedures are not always effective in creating a cooperative environment. In addition, the over-formalisation of the process may sometimes jeopardise policy-making. Therefore, what is really needed is formal and informal dialogue among the EU institutions, in particular between the European Parliament, the Commission and the Council. At the same time, the Fundamental Rights Agency and European Data Protection Supervisor should be given powers in the external dimension of data protection cooperation and if necessary, their competencies should be expanded to cover third-pillar matters.

Improvements to transparency and accountability would help the EU to consolidate its positions and would contribute to the emergence of a more coherent EU voice. While it would not prevent discussion about contentious points, it would at least facilitate the inclusion of more participants and views in the public debate. Consequently, we would avoid situations in which some actors are 'surprised' by decisions already taken, while reducing the possibilities for conflict.

5.3 Bridging private sector and non-governmental organisations

Another set of problems relates to the cooperation between the EU institutions and the private sector. Whereas the private sector benefits from wide access to policy-makers – a tendency likely to grow with the increasing use of new technologies and the greater level of public–private sector cooperation proposed in the Commission Communication[110] – the limited participation of non-governmental organisations in the policy-making process is problematic. Therefore, there is a clear need for a platform on which civil liberties organisations and government representatives can interact.

The case of EU–US homeland security proves the importance of dialogue for mutual learning and building trust. Unfortunately, often these groups (i.e. private-sector companies and non-governmental organisations) operate far too distinctly from one another, leading to the situation in which each speaks a different language. Such a fragmentation of positions within the EU further undermines the EU's position globally. Therefore, stimulating dialogue among existing

---

to mitigate those risks. See Department of Homeland Security (DHS), *Department of Homeland Security Privacy Office Annual Reports to the Congress, July 2007–July 2008*, DHS, Washington, D.C., 2008(a).

[109] Ibid.

[110] European Commission (2009), p. 8.

platforms or providing new opportunities would be desirable. For instance, initiatives such as the EU Framework Programmes could provide beneficial treatment and take advantage of integrated private–private initiatives in which private sector and non-governmental organisations (e.g. civil liberties organisations) submit joint project proposals or introduce peer review processes. In addition, the involvement of private actors and the academic community could provide impetus for further transatlantic integration and the development of the "transatlantic common space"[111] suggested by the Informal High-Level Advisory Group on the Future of European Home Affairs Policy (the Future Group). One format could be the establishment of a joint EU–US homeland security institute that would bring together major stakeholders from both sides of the Atlantic: scholars and practitioners in the field of law, security and trade from the US and from the EU. The analysis undertaken by particular teams in such an institute would provide the background and feed discussions between American and EU policy-makers, based on facts and objective analysis rather than political assessment alone. Such an institute would also closely cooperate with other stakeholders, including the Fundamental Rights Agency, the EU Data Protection Supervisor, the European Ombudsman and the Article 29 Working Party. This solution would further depoliticise the process and push the debate more towards content than emotions.

5.4 Towards a global approach to data protection

Given the scope of transatlantic cooperation in the field of homeland security and the extent to which the EU's policies borrow from solutions introduced in the US or in other countries (Canada or Australia), it would be advantageous to focus some efforts on working towards global solutions. For instance, several countries (as well as the EU) are working on the establishment of 'trusted traveller' programmes. Without coherence among these programmes or mutual recognition, citizens will be exposed to several systems, each based on its own merits. In such cases, a common system or mutual recognition agreements could prove valuable. An appropriate format for working towards such a system or agreement would be within the existing international organisations (i.e. IATA, ICAO, the OECD or Council of Europe). At the EU–US level, it could be done within a transatlantic homeland security agency, set up in a similar way as several other agencies in the EU. In view of the sensitivity of the issues at hand, it would not have any regulatory power but rather contribute to policy-making by providing information and studies. It would also contribute greatly to diminishing the workload of officials on both sides of the Atlantic.

[111] The report of the Future Group states that "consideration could further be given to a common transatlantic space with more sharing of relevant information and at the same time greater protection of personal data, expedited travel for bona fide passengers and more secure borders". See Future Group, *Freedom, Security and Privacy – European home affairs in an open world, Report of the Informal High-Level Advisory Group on the Future of European Home Affairs Policy*, Brussels, June 2008 (retrieved from www.statewatch.org).

Bibliography

Abbott, K.W. and D. Snidal (2001), "International 'standards' and international governance", *Journal of European Public Policy*, Vol. 8, No. 3, pp. 345-370.

Alegre, S. (2008), *The EU's External Cooperation in Criminal Justice and Counter-terrorism: An Assessment of the Human Rights Implications with a Particular Focus on Cooperation with Canada*, CEPS Special Report, CEPS, Brussels, September.

Andreas, P. (2002), "Re-bordering of America after 11 September", *Brown Journal of World Affairs*, Vol. 8, No. 2, pp. 195-202.

———— (2003), "Redrawing the Line: Borders and Security in the 21st Century", *International Security*, Vol. 28, No. 2, pp. 78-112.

Argomaniz, J. (2009), "When the EU is the 'norm-taker': The Passenger Name Records agreement and the EU's internalisation of U.S. border security norms", *Journal of European Integration*, Vol. 31, No. 1, pp. 119-136.

Article 29 Data Protection Working Party (2001), Opinion 10/2001 on the need for a balanced approach in the fight against terrorism, 0901/02/EN/Final, WP 53, Brussels, 14 December.

———— (2002), Opinion 6/2002 on transmission of passenger manifest information and other data from airlines to the United States, 11647/02/EN, WP 66, Brussels, 24 October.

———— (2003), Opinion 4/2003 on the level of protection ensured in the US for the transfer of passengers' data, 11070/03/EN, WP 78, Brussels, 13 June.

———— (2004), Opinion 2/2004 on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, Brussels, WP 87, 29 January.

Bigo, D. (2008), "Globalized (in)Security: The Field and the Ban-opticon", in D. Bigo and A. Tsoukala (eds), *Terror, Insecurity and Liberty*, London: Routledge, pp. 10-48.

Bigo, D. and S. Carrera (2007), *From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU*, CEPS Commentary, CEPS, Brussels, 17 February (retrieved from http://ceps01.link.be/Article.php?article_id=314).

Bigo, D., S. Carrera, E. Guild and R.B.J. Walker (2007), *The changing landscape of European liberty and security: Mid-term report on the results of the CHALLENGE project*, CHALLENGE Research Paper No. 4, CEPS, Brussels, February.

CERI/Sciences Po-CNRS CHALLENGE Research Group (2008), "Mapping of the European Security Agencies", CERI/Sciences Po-CNRS, Paris (retrieved from www.libertysecurity.org/article1670.html).

Council of the European Union (1995), Directive 95/46/EC 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.

———— (2002), Consolidated version of the Draft Supplemental Agreement between the United States of America and Europol on the exchange of personal data and related information, 15231/02, Brussels, 5 December.

———— (2004), Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ L 183, 20.05.2004.

———— (2006), Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the Undertakings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of Passenger Name Record (PNR) data, 13738/06, Brussels, 11 October.

———— (2006), Reply by the Council Presidency and the Commission to the letter from the USA's Department of Homeland Security, 13835/06, Brussels, 13 October.

———— (2007a), Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204, 04.08.2007.

———— (2007b), Processing of EU-originating Personal Data by United States Treasury Department for Counter-Terrorism Purposes – 'SWIFT', 10741/2/07 REV 2, Brussels, 29 June.

———— (2008a), Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008.

———— (2008b), *Final Report by EU–US High-Level Contact Group on information sharing and privacy and personal data protection,* 9831/08, Brussels, 28 May.

———— (2009), Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5618/09, Brussels, 23 January.

Cox, P. (2004), Statement concerning the decision of the European Parliament to go to court over Council and Commission decisions on PNR data agreement with USA, European Parliament, 25 June (retrieved from http://www.statewatch.org/news/2004/jun/21-ep-court-pnr.htm).

Crosbie, J. (2009), "Commission to seek new deal with the US on data transfers", *European Voice*, 16 July.

Department of Homeland Security (DHS) (2004a), Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP), DHS, Washington, D.C., 11 May.

———— (2004b), Transcript of Secretary of Homeland Security Tom Ridge, DHS, Washington, D.C., 30 November (retrieved from http://www.dhs.gov/xnews/releases/press_release_0562.shtm).

———— (2008a), *Department of Homeland Security Privacy Office Annual Reports to the Congress, July 2007–July 2008*, DHS, Washington, D.C.

———— (2008b), Statement on Information Sharing and Privacy and Personal Data Protection between the European Union and the United States of America, DHS, Washington, D.C., 12 December (retrieved from http://www.dhs.gov/xabout/international/gc_1229359375601.shtm#0).

Djelic, M.L. (2004), "Social networks and country-to-country transfer: Dense and weak ties in the diffusion of knowledge", *Socio-Economic Review,* Vol. 2, pp. 341-370.

Djelic, M.L. and K. Sahlin-Andersson (eds) (2007), *Transnational governance: Institutional dynamics of regulation*, Cambridge: Cambridge University Press.

European Commission (2003), European Commission/U.S. customs talks on PNR transmission: Joint statement, Brussels, 17-18 February.

————— (2004), Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection, OJ L 235, Brussels, 06.07.2004.

————— (2007), "Fight against terrorism: Stepping up Europe's capabilities to protect citizens against the threat of terrorism", IP/07/1649, Brussels, 6 November.

————— (2008), Communication on preparing the next steps in border management in the European Union, COM(2008) 69 final, Brussels, 13 February.

————— (2009), Communication on an Area of Freedom, Security and Justice serving the citizen, COM(2009) 262 final, Brussels, 10 June.

European Parliament (2003a), Resolution on transfer of personal data by airlines in the case of transatlantic flights: State of negotiations with the USA, P5_TA-PROV(2003)0429, 8 October.

————— (2003b), Transmission of personal data by airlines in the case of transatlantic flights, European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: State of negotiations with the USA, P5_TA-PROV(2003)0429, 9 October.

————— (2004), Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection, 2004/2011(INI), P5_TA-PROV(2004)0245.

————— (2008), *Data protection from a transatlantic perspective: The EU and US move towards an international data protection agreement?*, PE 408.320, Directorate-General for Internal Policies of the Union, Brussels, October.

Flynn, S.E. (2000), "Beyond Border Control", *Foreign Affairs*, Vol. 79, No. 6.

Future Group (2008), *Freedom, Security and Privacy – European home affairs in an open world, Report of the Informal High-Level Advisory Group on the Future of European Home Affairs Policy*, Brussels, June (retrieved from www.statewatch.org).

Guild, E. (2003), "International terrorism and EU immigration, asylum and border policy: The unexpected victims of 11 September 2001", *European Foreign Affairs Review*, Vol. 8, No. 3, pp. 331-346.

————— (2006), "The judicialisation of armed conflict: Transforming the twenty-first century", in J. Huysmans, A. Dobson and R. Prokhovnik (eds), *The politics of protection, sites of insecurity and political agency*, London: Routledge.

Guild E. and E. Brouwer (2006), *The political life of data: The ECJ decision on the PNR Agreement between the EU and the US*, CEPS Policy Brief No. 109, CEPS, Brussels, July.

Guild, E. and S. Carrera (2009), *Towards the next phase of the EU's Area of Freedom, Security and Justice: The European Commission's proposals for the Stockholm Programme*, CEPS Policy Brief No. 196, CEPS, Brussels, 20 August.

Guild, E., S. Carrera and A. Faure-Atger (2009), *Challenges and prospects for the EU's Area of Freedom, Security and Justice: Recommendations to the European Commission for the Stockholm Programme*, CEPS Working Paper No. 313, CEPS, Brussels, April.

Guild, E., S. Carrera and F. Geyer (2008), *The Commission's new border package. Does it take us one step closer to a 'cyber-fortress Europe'?*, CEPS Policy Brief No 154, CEPS, Brussels, March.

Hobbing, P. (2008), *Tracing Terrorists: The EU–Canada Agreement in PNR Matters*, CEPS Special Report, CEPS, Brussels (revised version), 17 November.

Koslowski, R. (2004), *International cooperation to create smart borders*, Woodrow Wilson International Center for Scholars, Washington, D.C.

Lazer, D. (2001), "Regulatory interdependence and international governance", *Journal of European Public Policy*, Vol. 8, No. 3, pp. 474-492.

Moiny, Y. (2005), *Protection of personal data and citizens' rights of privacy in the fight against the financing of terrorism*, CEPS Policy Brief No. 67, CEPS, Brussels, March.

National Commission on Terrorist Attacks upon the United States (2004), *The 9/11 Commission report: Final report of the national commission on terrorist attacks upon the United States*, New York: W.W. Norton and Company.

Nicolaidis, K. and M.P. Egan (2001), "Transnational market governance and regional policy externality: Why recognize foreign standards?", *Journal of European Public Policy*, Vol. 8, No. 3, pp. 454-473.

Pawlak, P. (2007a), "From Hierarchy to Networks: Transatlantic Governance of Homeland Security", *Journal of Global Change and Governance*, Vol. 1, No. 1.

———— (2007b), "Transatlantic border and transport security cooperation: Can one swallow make a summer?", in D. Hansen and M. Ranstorp, *Cooperating against terrorism: EU–US relations post September 11*, National Defence College, Stockholm.

———— (2009a), "The External Dimension of Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization?", *Journal of European Integration*, Vol. 31, No. 1, pp. 25-44.

———— (2009b), "Network politics and transatlantic homeland security cooperation", *Perspectives on European Politics and Society*, Vol. 10, No. 4, Special Issue, forthcoming in December.

Peterson, J., H. Wallace, M.A. Pollack, R. Doherty, F. Burwell, J.P. Quinlan and A. Young (2005), *Review of the framework for relations between the European Union and the United States: An independent study*, European Commission, Brussels.

Ring, P.S. and A.H. Van De Ven (1994), "Developmental processes of cooperative interorganisational relationships", *Academy of Management Journal*, Vol. 19, No. 1, pp. 90-118.

Rosenzweig, P. (2007), "Seven questions for the European Union", *Privacy & Security Law Report*, Vol. 6, No. 46.

Salter, M.B. (2005), "At the Threshold of Security: A Theory of Borders", in M.B. Salter and E. Zureik (eds), *Global Surveillance and Policing: Borders, Security, Identity*, New York: Willan Publishing, pp. 36-50.

———— (2009), "Borders, Passports, and the Global Mobility Regime", in B.S. Turner (ed.), *Handbook of Globalization Studies*, London: Taylor and Francis.

Scandamis, N., F. Sigalas and S. Stratakis (2007), *Rival freedoms in terms of security: The case of data protection and the criterion of connexity*, CHALLENGE Research Paper No. 7, CEPS, Brussels, December.

Statewatch (2007), "EU/US security 'channel' – A one-way street?", *Statewatch Bulletin*, Vol. 17, No. 1.

The White House (2002a), *Smart Borders for the 21st Century*, Office of the Press Secretary, Washington, D.C., 25 January (retrieved from http://usinfo.state.gov/is/Archive_Index/Border_Security_Smart_Borders_for_the_21st_Century.html).

———— (2002b), *National Strategy for Homeland Security*, Office for Homeland Security, Washington, D.C., July.

Tsoukala, A. (2008), *Security, Risk and Human Rights: A vanishing relationship?*, CEPS Special Report, CEPS, Brussels, September.

US Mission to the European Union (2004), *U.S., EU discuss transportation, border security*, Brussels, 27 April (retrieved from http://useu.usmission.gov/Article.asp?ID=3B93FC1F-F30E-467D-A287-54777BE14CE7).