Social Sciences Research Centre
Institute for European Integration Research

OAW
Austrian Academy of Sciences

Institute for European Integration Research

Working Paper Series

Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement

Marise Cremona

Working Paper No. 04/2011
March 2011

Institute for European Integration Research
Strohgasse 45/DG
1030 Vienna/Austria
Phone: +43-1-51581-7565
Fax: +43-1-51581-7566
Email: eif@oeaw.ac.at
Web: www.eif.oeaw.ac.at

Abstract

The EU's policy on Justice and Home Affairs has as its objective the establishment of the Union as 'an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States'. How does this essentially internal objective translate into international action? How does the Union respond, in an internal policy field, to external challenges?

This paper will assess the ambitions and the reality of the external dimension of the EU's policy of Justice and Home Affairs from two perspectives. The first is the close *link between internal and external objectives and policies*, and the implications for both EU competence and policy priorities. The second is the *progressive constitutionalisation* of the JHA field, its transformation from inter-governmental cooperation into a policy domain subject to the political and judicial accountability of ordinary legislative procedures.

The paper is structured around a case study of the negotiation, renegotiation and eventual conclusion of the EU-US Agreement on the transfer of financial messaging data for the purpose of combating terrorism (the 'SWIFT' Agreement), and in particular the *interplay* thereby revealed between

(i) different *regulatory approaches* to data protection in the context of international commercial transactions and the needs of private commercial undertakings;

(ii) different (EU) *institutional actors* in the context of international action against terrorism where the EU needs to be seen as an effective actor and partner of the US; and

(iii) the needs of *public security* and the need to provide against the risk of breaches of *individual rights* of data protection and privacy through the misuse of security-based powers.

Contents

Abbreviations

AFSJ	Area of Freedom, Security and Justice
EDPS	European Data Protection Supervisor
FMDA	Financial Messaging Data Agreement
ISS	Internal Security Strategy
JHA	Justice and Home Affairs
LIBE Committee	European Parliament Committee on Civil Liberties, Justice and Home Affairs
PNR	Passenger Name Records
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Programme

1. INTRODUCTION

The EU's policy on Justice and Home Affairs has as its objective the establishment of the Union as 'an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States'.[1] How does this essentially internal objective translate into international action? How does the Union respond, in an internal policy field, to external challenges?

The Stockholm Programme for Justice and Home Affairs, adopted by the European Council in December 2009, emphasises the importance of its external dimension: it is, the Programme says, 'essential to address the key challenges we face' and is 'crucial to the successful implementation of the objectives of this programme'.[2] And indeed the area of freedom, security and justice has been one of the most active domains of EU external relations over the last decade.[3] The EU has concluded agreements establishing arrangements with neighbouring states on border management[4] and on asylum,[5] and a number of agreements on readmission[6]

[1] Article 67(1) Treaty on the Functioning of the European Union (TFEU). The term 'Area of Freedom, Security and Justice' (AFSJ) corresponds to the name given to Title V of Part III of the TFEU. The term 'Justice and Home Affairs' is not found as such in the Treaties; however it is a more familiar and recognisable term and it also represents the Commission's choice of labels for its two Directorates General in this policy field: Justice (which includes fundamental rights and citizenship and is currently headed by Commissioner Reding) and Home Affairs (which includes migration, security and in particular terrorism and organised crime, and civil protection/ emergencies, and which is currently headed by Commissioner Malmström). These two DGs replaced the single DG Justice, Freedom and Security (known as JLS from its French acronym) in 2010.

[2] The Stockholm Programme – An open and secure Europe serving and protecting the citizens, adopted by the European Council 11-12 December 2009, Council doc. 17024/09. The Programme covers 2010-2014. See also Communication from the Commission to the European Parliament and the Council, 'An area of freedom, security and justice serving the citizen' COM (2009) 262, 10 June 2009.

[3] On the external dimension of the area of freedom security and justice generally, see G De Kerchove and A Weyembergh (eds), *Securite et Justice: Enjeu de la Politique Exterieure de l'Union Europeenne*, Brussels, editions ULB, 2003; J Monar, 'The EU as an international actor in the domain of justice and home affairs' (2004)9 *European Foreign Affairs Rev.* 395; B Martenczuk and S Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations*, VUBPress 2008; S Wolff, N Wichmann and G Mournier (eds), (2009) 31 *Journal of European Integration* 'Special Issue: The External Dimension of Justice and Home Affairs? A Different Security Agenda for the EU'; M Cremona, J Monar and S Poli (eds), *The External Dimension of the Area of Freedom, Security and Justice*, Peter Lang-P.I.E, forthcoming 2011.

[4] For example, agreements with Iceland, Norway, Switzerland and Liechtenstein on their participation in the European Agency for the Management of Operational Cooperation at the External Borders of the EU Member States (Frontex).

[5] For example, the Agreement between the European Community, the Swiss Confederation and Liechtenstein concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland.

[6] Agreements have been concluded inter alia with Albania, the Former Yugoslav Republic of Macedonia, the Republic of Montenegro, the Republic of Serbia, Bosnia and Herzegovina, Russia, Ukraine, Sri Lanka, Macao and Hong Kong.

and visa facilitation.[7] It has acceded to the Hague Conference on Private International Law[8] and signed the Hague Convention on Choice of Court Agreements.[9] It has concluded the revised Lugano Convention on jurisdiction and enforcement of judgments in civil and commercial matters, and a number of other conventions in the field of private international law. It has concluded bilateral agreements on mutual legal assistance and extradition with the USA,[10] several multilateral Conventions on organised crime, trafficking and terrorism[11] and a cooperation agreement with the International Criminal Court.[12] Specific provisions on cooperation in justice and home affairs are now included in association and cooperation agreements.[13] Although some of these agreements are mixed (concluded by the Union and Member States together), very many of them are concluded by the EU acting alone.

It is clear that international cooperation is an essential aspect of this policy field.[14] The threats identified by the Internal Security Strategy (ISS) adopted in March 2010[15] (terrorism, serious and organised crime, cyber-crime, natural and man-made disasters) are not threats which respect the EU's external borders and it is not surprising that the ISS argues that internal security increasingly depends to a large extent on external security, that the concept of internal security cannot exist without an external dimension. External and internal

---

[7] See for example Council Decision 2007/827/EC on the conclusion of the Agreement between the EC and Moldova, OJ 2007 L 334/168. Similar agreements have been concluded with Ukraine, Russia, Albania, Bosnia and Herzegovina, Montenegro, Serbia, the former Yugoslav Republic of Macedonia.

[8] Council Decision 2006/719/EC on the accession of the Community to the Hague Conference on Private International Law OJ 2006 L 297/1.

[9] Council Decision 2009/397/EC on the signing on behalf of the European Community of the Convention on Choice of Court Agreements OJ L 133, 29.5.2009, p. 1.

[10] Council Decision 2003/516/EC concerning the signature of the Agreements between the EU and the USA on extradition and mutual legal assistance in criminal matters OJ 2003 L/25. See further V Mitsilegas 'The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data' (2003) 8 *European Foreign Affairs Rev*, 515.

[11] For example the UN Convention against Transnational Organized Crime (Palermo Convention), concluded for the EC by Decision 2004/579/EC of 29 April 2004 OJ 2004 L 261/69.

[12] Council Decision 2006/313/CFSP of 10 April 2006 concerning the conclusion of the Agreement between the International Criminal Court and the European Union on cooperation and assistance, OJ 2006 L 115/49.

[13] For example the Stabilisation and Association Agreements with Albania, Croatia, Macedonia, Montenegro and Serbia; these contain provisions on justice and rule of law cooperation (including independence of judiciary and improving police), data protection, cooperation on visas, border management, asylum and migration, control of illegal immigration, readmission, and cooperation on money laundering, terrorism financing, illicit drugs, counter-terrorism and on organised and serious crime including smuggling and trafficking in human beings, counterfeiting, corruption, smuggling and arms trafficking.

[14] Commission Communication 'A Strategy on the External Dimension of the Area of Freedom, Security and Justice' COM(2005)491 of 12 October 2005; Council Strategy for the External Dimension of the Area of Freedom, Security and Justice, adopted December 2005, Council Doc. 14366/3/05.

[15] Internal Security Strategy for the European Union: "Towards a European Security Model" adopted by the European Council 25-26 March 2010, see Council doc. 7120/10.

dimensions of security are inter-dependant and a 'global security approach' with third countries is advocated:

> The EU must not restrict itself just to cooperation between the law-enforcement agencies of Member States and other countries, especially EU neighbours. It is necessary to build relationships with other countries through a global approach to security, working closely with them and, when necessary, supporting their institutional, economic and social development. This system of working will mean establishing opportunities for dialogue through areas of mutual interest, concerns and the possibilities for cooperation that can be identified in each case. Cooperation and coordination with international organisations in the field of law enforcement, in particular with Interpol, should be enhanced.[16]

In its Conclusions on the Commission's Action Plan for the ISS in February 2011, the Council summarized its view of the *European Security Model*:

> [T]he European Security Model, as defined by the Internal Security Strategy … should be based on a shared agenda for action, an appropriate balance between prevention and tackling the consequences of threats to security, the development of security policies based on common values and a renewed effort to establish closer links between the external and internal aspects of EU security and to promote initiatives designed to strengthen the capacity for action of third countries.[17]

These are the ambitions. What of the reality? Before we turn to the specific example that I should like to explore today, let me first briefly mention three characteristics of the external dimension of the EU's area of freedom, security and justice (AFSJ).[18]

The first is in fact an aspect of the link between the internal and the external just mentioned in the context of the security strategy. External competence as regards the area of freedom, security and justice is almost entirely an implied competence – meaning that there is no explicit Treaty reference to external action or international relations. There are now two explicit provisions, both in the chapter on borders, asylum and migration, which reflect pre-existing practice based on implied powers.[19] All other external action is implied and this means that a specific case needs to be made for the necessity for Union action; it is not

[16] Internal Security Strategy, note 15 above, p.16.

[17] Council conclusions on the Commission communication on the European Union internal security strategy in action, 21 February 2011, Council doc. 6699/11.

[18] See further M Cremona, 'EU External Action in the JHA Domain: A Legal Perspective' in M Cremona, J Monar and S Poli (eds), note 3 above.

[19] Article 78(3) TFEU provides that the Union's common asylum system may include partnership and cooperation with third countries for the purpose of managing asylum applications or temporary protection; and Article 79(3) TFEU provides an explicit legal basis for readmission agreements.

automatic. Implied competence is deeply connected to Treaty objectives.[20] It flows from measures adopted by the Union in order to achieve (internal) objectives:

> 'The competence of the Community to conclude international agreements may arise not only from an express conferment by the Treaty but may equally flow implicitly from other provisions of the Treaty and from measures adopted, within the framework of those provisions, by the Community institutions … [W]henever Community law created for those institutions powers within its internal system for the purpose of attaining a specific objective, the Community had authority to undertake international commitments necessary for the attainment of that objective even in the absence of an express provision to that effect.'[21]

Where a Union objective can be derived from the Treaty, for the attainment of which internal powers have been granted, these may be complemented where necessary by external powers. Thus in this Justice and Home Affairs policy field we do not see independent *external objectives*: the external action must be necessary to achieve the *internal objectives* established by the Treaty. The inter-dependence of the internal and the external is not only a matter of pragmatic fact, therefore, but built into the legal nature of the policy.

Second, this is a policy area where competence is shared between the Union and the Member States. Power is not per se exclusive to the Union, which operates alongside its Member States, although once the Union has acted, its competence may become exclusive through pre-emption.[22] As a consequence of shared competence, if an international agreement is envisaged, it needs to be shown that neither internal EU action nor bilateral Member State action will fulfil the relevant objectives. And indeed in discussing the external dimension of the AFSJ, the institutions have emphasised the importance of what they call the 'value added' of EU action. This is a more direct way of expressing the concept of subsidiarity found in Article 5(3) TEU.[23]

---

[20] See further M Cremona, 'Defining Competence In EU External Relations: Lessons from the Treaty Reform Process' in A. Dashwood and M. Maresceau (eds.) *Law and Practice of EU External Relations – Salient Features of a Changing Landscape*, Cambridge University Press, 2008.

[21] Opinion 1/2003 of 7 February 2006 on the Lugano Convention, [2006] ECR I-1145, para 114. Note that since the coming into force of the Treaty of Lisbon, on 1 December 2009, 'Community' should be read as 'Union'.

[22] Article 2(2) TFEU. This was the case, for example, for the revised Lugano Convention: Opinion 1/03, note 21 above.

[23] According to Article 5(3) TEU, 'Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States … but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.' For a recent example of the emphasis on added value, see the JHA Council Conclusions of 24-25 February 2011 on the Commission's Action Plan for the Internal Security Strategy, Council doc. 7012/11.

The third aspect of the Union's competence in this field relates to its constitutional evolution. The Union's first involvement in justice and home affairs issues was through the so-called third pillar, introduced by the Treaty of Maastricht. The Treaty of Amsterdam brought certain aspects, relating to migration and to civil justice, into the EC Treaty but criminal justice cooperation remained in the TEU. The Treaty of Lisbon has reunited the different dimensions of the policy under the Title on the Area of Freedom, Security and Justice and with one or two exceptions[24] the normal institutional and legislative procedures apply to this Title. The transition from the former third pillar has some important implications, in particular relating to the jurisdiction of the Court of Justice[25] and the increased role given to the European Parliament. [26]

With these three characteristics of the EU's justice and home affairs policy in mind, let us turn to the particular example I have chosen to illustrate some of the difficulties the EU has in translating its ambition into reality. We are going to examine the negotiation, renegotiation and eventual conclusion of the EU-US Agreement on the transfer of financial messaging data for the purpose of combating terrorism (the 'SWIFT' Agreement). This is one aspect of a wider issue: international (and in particular transatlantic) transfers of data for purposes of combating terrorism and organised crime, and the implications these pose for the protection of fundamental rights.[27] There are three chapters in this story which each shed light on a different dimension of EU policy-making.

First, the need for *external action by the EU* arising from different regulatory approaches to data protection in the context of international commercial transactions and the needs of private commercial undertakings: the value added principle at work (II).

Second, the impact of the constitutional change introduced by the Treaty of Lisbon on the relations between different EU institutional actors, in the context of international action

[24] For example, the special legislative procedure applied to measures concerning family law by Article 81(3) TFEU, and the 'emergency brake' available in the case of proposals to establish minimum rules on criminal procedure and criminal offences by Articles 82(3) and 83(3) TFEU.

[25] See K Lenaerts, 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' (2010) 59 *International and Comparative Law Quarterly* 255.

[26] On constitutional change in the AFSJ, see J Monar, 'Justice and Home Affairs in the EU Constitutional Treaty. What Added Value for the Area of Freedom, Security and Justice?' (2005) 1 *European Constitutional Law Rev*, 226.

[27] See generally P de Hert and B de Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT' in B Martenczuk and S Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations*, VUBPress 2008; V Papakonstantinou and P de Hert, 'The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic' (2009) 46 *Common Market Law Rev* 885.

against terrorism where the EU needs to be seen as an effective actor and partner of the US (III).

Third, the relationship between the needs of public security and the need to provide against the risk of breaches of individual rights of data protection and privacy through the misuse of security-based powers: a test for the European Security Model promoted by the Internal Security Strategy which declares its commitment to 'mutually reinforcing' justice, freedom and security policies which respect fundamental rights, international protection, the rule of law and privacy[28] (IV).

[28] Internal Security Strategy, note 15 above, p.9.

2. THE FIRST CHAPTER: LEGAL UNCERTAINTY AND THE NEED FOR AN EU RESPONSE

SWIFT is the Society for Worldwide Interbank Financial Telecommunication, a member-owned cooperative. According to its own information, more than 9,000 banking organisations, securities institutions and corporate customers in 209 countries use SWIFT every day to exchange standardised financial messages. SWIFT is based in Belgium but has offices in 20 countries, including the USA.

After 11 Sept 2001, the US instituted the Terrorist Finance Tracking Program (TFTP). The TFTP is part of the US response to UN Security Council Resolution 1373 (2001). Under the TFTP, the US Treasury Department issued subpoenas for financial information to (among others) SWIFT's Operating Centre in the United States. The US Centre had servers which 'mirrored' (contained the same information as) the EU-based SWIFT servers and thus the US Treasury Department was able to order SWIFT to supply it with information on financial transfers between EU subjects.

In June 2006, US newspapers revealed the existence of the TFTP and there was much comment about privacy. It was revealed that the SWIFT subpoenas covered European transactions and concerns were expressed in the European Parliament that EU data protection legislation (especially Directive 95/46/EC[29]) was not being complied with. Transfers to the US need to comply with EU Safe Harbour principles.[30] SWIFT itself was unhappy about the legal uncertainty of compliance with EU data protection laws, and their TFTP obligations, and with some reason: on 27 July 2006 the Belgian Data Protection Authority issued an opinion that SWIFT activities were in breach of Belgian Data Protection Law, which implements the EU Data Protection Directive.

In November 2006 the 'Article 29 Working Party' (the European Commission's independent advisory body on data protection and privacy) issued an opinion on the processing of personal data by SWIFT. Its view was that SWIFT was in breach of Community data protection law in transferring personal data to the US (i) without ensuring adequate protection and (ii) without giving individuals information about how their data might be used. The European Parliament adopted two Resolutions on SWIFT in 2006 and 2007,

[29] Directive 95/46/EC of the European Parliament and of the Council 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, p. 31.

[30] The Commission Decision on safe harbour privacy principles establishes these; transfers to US are compliant only if made to companies which agree to comply with the Safe Harbour principles: Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles OJ L 215, 25.8.2000, p. 7.

referring to the fact that 'businesses with operations on both sides of the Atlantic increasingly find themselves caught between the conflicting legal requirements of the US and EC jurisdictions', and calling for an agreement with the USA to resolve the existing legal uncertainty as to data protection guarantees.[31]

What was the response? Initially it was 'soft', in other words an attempt at reassurance over compliance with EU standards rather than a binding agreement. On 28 June 2007 the US Treasury sent the EU Council and Commission 8 pages of 'Representations' outlining the operation of the TFTP and how its demands from SWIFT and its handling of the data received meet European data protection concerns.[32] It stressed the importance of financial information in tracking terrorism. It said the data was used only in connection with specific information on terrorist activity (no data mining or general searches) and only in connection with terrorism (no other unlawful activity such as drug trafficking or tax evasion). Unextracted data was deleted after five years. It set out the legal basis for the TFTP in US law. The US also agreed to the appointment of an 'eminent European person' to assess the TFTP controls:

> 'As a sign of our commitment and partnership in combating global terrorism, an eminent European person will be appointed to confirm that the program is implemented consistent with these Representations for the purpose of verifying the protection of EU-originating personal data. In particular, the eminent person will monitor that processes for deletion of non-extracted data have been carried out. The eminent person will have appropriate experience and security clearances, and will be appointed for a renewable period of two years by the European Commission in consultation with the Treasury Department. The eminent person shall act in complete independence in the performance of his or her duties.'

In December 2008 the Belgian data protection Authority issued a report confirming that in dealing with the TFTP subpoenas SWIFT now complied with Belgian data protection law. In March 2008 Judge Jean-Louis Bruguière was appointed by the Commission as the 'eminent European person' and he made an initial report in January 2009: this was reported to the European Parliament Civil Liberties, Justice and Home Affairs (LIBE) Committee in February 2009.[33] The report confirmed compliance by the TFTP with the US Representations. A second and final report was produced in early 2010.

---

[31] Resolution of 6 July 2006 on the interception of bank transfer data from the SWIFT system by the US secret services (OJ C 303 E, 13.12.2006, p. 843); Resolution of 14 February 2007 on SWIFT, the PNR agreement and the transatlantic dialogue on these issues (OJ C 287 E, 29.11.2007, p. 349).

[32] OJ 2007 C 166/18. For the Council's response to this, see Council doc. 11291/2/07 REV 2 (Presse 157), 28 June 2007.

[33] IP/09/264, 17 Feb 2009.

At this stage, then, it was a matter of ensuring that the transfers within the USA made under subpoena by SWIFT to the US Treasury Department complied with the Union's Data Protection requirements, and in particular its Safe Harbour Principles. The results of the negotiations between the EU Commission and Council with the US Treasury were a series of undertakings on the US side, with some EU oversight of compliance. However this was not the end of the story.

From 1 January 2010 SWIFT altered its systems so that all the data concerning intra-European transactions is now held in two European sites and is no longer mirrored in the USA (a change first announced in October 2007). This would mean that its EU-based data is no longer covered by US law (or the TFTP subpoenas) and transfers of the EU data to the TFTP would no longer take place. The EU Council and Commission were concerned both because they wanted to demonstrate cooperation with the US on counter-terrorism and because EU governments receive a substantial amount of information from the TFTP, based on analysis of European records: there is at present no TFTP equivalent in the EU so the EU relies on the US processing of the data. In order to ensure that data would continue to be transferred from the EU to the US, on 27 July 2009 the Council authorised the Presidency, assisted by the Commission, to open negotiations for an Agreement on Financial Messaging Data between the EU and the USA (the FMDA). The Agreement would allow the US Treasury Department to serve production orders on designated data providers, including SWIFT. Here then we see the value added principle at work. The action by SWIFT made a formal agreement between the EU and US necessary, an agreement which – it was envisaged – would both require the transfers from Europe and meet EU data protection concerns.

3. THE SECOND CHAPTER: CONSTITUTIONAL CHANGES

The proposed agreement was controversial and its history became linked to the coming into force of the Treaty of Lisbon and the changes that brought to decision-making in Justice and Home Affairs. It will be remembered that in 2007, following legal action by the European Parliament, the EU-US agreement on the transfer of passenger name records (PNR) for law enforcement purposes had been renegotiated as a third pillar agreement.[34] It was now proposed that the EU-US FMDA, as a law enforcement measure, would also be negotiated and concluded under the third pillar.[35] But this was mid-2009 and the Treaty of Lisbon – which would abolish the third pillar – was to come into force on 1 December.

On 17 September 2009 the European Parliament passed a Resolution on the proposed FMDA.[36] The Parliament commented on the fact that neither the negotiating directives nor the opinion of the Council's Legal Service on choice of legal basis were publicly available since they were classified as 'restricted', as well as on the fact that the proposed agreement would be fully provisionally applicable upon signature. While reaffirming its support for the fight against terrorism, it also mentions 'the need to strike the right balance between security measures and the protection of civil liberties and fundamental rights, while ensuring the utmost respect for privacy and data protection,' and the risk that the data could be 'misused for large-scale forms of economic and industrial espionage'. The Parliament asked why Article 4 of the EU-US agreement on mutual legal assistance,[37] which provides for the transfer of specific financial data on request, could not be used instead of an agreement on SWIFT, which provided for bulk transfers of data. It set out a series of minimum conditions that the agreement should comply with, including:

- that data are transferred and processed only for the purposes of fighting terrorism, as defined in the 2002 Framework Decision on combating terrorism,[38] and that they relate to individuals or terrorist organizations recognised as such by the EU;
- that the transfer requests are based on specific, targeted cases;

---

[34] Joined Cases C-317/04 and C-318/04 *European Parliament v Council* [2006] ECR I-4721.

[35] In 2006, as we have seen, the issue was dealt with in the framework of the Data Protection Directive and the Commission's Safe Harbour (Adequacy) Decision of 2000. This was possible, even in the light of the judgment in cases C-317 and 318/94, note 34 above, since at this time the data was transferred from the EU to the USA by SWIFT for purely commercial purposes; the law enforcement requisition of the data took place within the USA (c.f. also case C-301/06 *Ireland v European Parliament and Council* [2009] ECR I-00593). However from 2010, when SWIFT no longer stored their EU data in the USA, the transfers to the US of EU data would be made solely for law enforcement purposes: hence the applicability of the Treaty provisions on police cooperation.

[36] P7_TA(2009)0016.

[37] See note 10 above.

[38] Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ 2002 L 164/3.

- that EU citizens and enterprises are granted defence rights, procedural guarantees and the rights of access to justice equivalent to those existing in the EU;
- a reciprocity mechanism, obliging the US authorities upon request to transfer relevant financial messaging data to the competent EU authorities;
- the inclusion of a sunset clause in the interim agreement; and the negotiation of a possible new agreement under the new EU legal framework that fully involves the European Parliament.

On 30 November 2009 – the day before the entry into force of the Treaty of Lisbon – the Council authorised the Presidency to sign an interim agreement between the European Union and the United States on the processing and transfer of Financial Messaging Data from the EU to the US for purposes of the Terrorist Finance Tracking Program (TFTP).[39] Like the 2007 PNR agreement, its legal basis was former Articles 24 and 38 TEU; it could therefore be signed by the Council alone without European Parliamentary consent.[40] The FMDA was to have been applied provisionally (that is, before its formal conclusion) from 1 February 2010. The Agreement had a maximum duration of 9 months and was to be replaced in due course by a longer term agreement.

On 17 December 2009 the Commission adopted a proposal for a Council decision concluding the FMDA.[41] With the coming into force of the Lisbon Treaty, the legal bases changed and the new JHA legal bases specify the ordinary legislative procedure for the adoption of internal acts (the agreement being concluded under implied powers). As a result the consent of the European Parliament is required under Article 218 (6)(a)(v) TFEU.

In early February 2010 the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) recommended the rejection of the agreement.[42] The LIBE

[39] Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program OJ 2010 L 8/9.

[40] A particular feature of (then) Article 24 TEU, which formed the legal basis for the signature authorising signature of the FMDA, was that although the European Parliament was not involved, national parliaments might well be: under paragraph 5, 'No agreement shall be binding on a Member State whose representative in the Council states that it has to comply with the requirements of its own constitutional procedure; the other members of the Council may agree that the agreement shall nevertheless apply provisionally.'

[41] Com (2009) 703. The legal bases proposed by the Commission were Articles 82(1)(d) and 87(2)(a) TFEU.

[42] Committee on Civil Liberties, Justice and Home Affairs, Recommendation on the proposal for a Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (05305/1/2010REV – C7-0004/2010 – 2009/0190(NLE)), Rapporteur: Jeanine Hennis-Plasschaert, 5 February 2010, A7-0013/2010.

Committee report was in favour of an agreement in principle, finding that the 'soft' guarantees in the US 'Representations' were not good enough. It was however unhappy that the agreement had effectively crystallized as a permanent arrangement something that was originally introduced as an emergency measure in the aftermath of 11 September 2001. It argued that the TFTP 'must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records.' The debate was about 'the law enforcement use of data collected for commercial purposes' and 'accepting the proposed FMDA (as it stands) could lead down the slippery slope of accepting other requests for commercial data with (f.e.) Skype, PayPal and other companies in the information-telecommunication field being potentially interesting for law enforcement purposes.' The Committee was concerned about mass transfers of data, about the absence of judicial authorisation, about the absence of controls over further transfer by the US to third countries, about the lack of information on the period for which extracted information was to be kept, the gaps in protection (access and redress) for European individuals and companies in the US, and the absence of true reciprocity (no EU access to US data). The Committee also complained of the failure to give the Parliament full information, including the Council's legal opinion and the reports by Judge Bruguière; it argued that this was a breach of the duty of sincere cooperation between EU institutions. It recommended that the Commission should propose a negotiating mandate for new agreements with the US on both financial messaging data for counter-terrorism investigations and privacy/personal data protection in the context of the exchange of information for law enforcement purposes (such as PNR).

The European Parliament was especially angry about the lack of consultation on the FMDA. Home Affairs Commissioner Malmström spoke in the Parliament, arguing that 'rejection of the Interim Agreement by this House would represent a serious blow to EU security', but this was not enough. In an unusual move, the Council issued a Declaration the day before the European Parliament vote, pointing out that the interim agreement was to last only 9 months, that it contained many of the features called for in the Parliament's Resolution of 17 September 2009, that a longer-term agreement would be negotiated and requesting the Commission to adopt that very month a draft mandate for a new agreement, that the European Parliament would play a full part in those negotiations, that it recognised the need for the European Parliament to have access to restricted information and committing itself to negotiating an inter-institutional agreement on this issue.[43]

[43] Council doc. 6265/10 (Presse 23), 9 February 2010.

Despite all these assurances, in a plenary vote in the European Parliament on 10 February 2010 the agreement was indeed rejected. The negative vote by the Parliament meant that the provisional application of the agreement was no longer possible. A letter from the Council Presidency was sent on 22 February to the US Secretary of State, stating that following the European Parliament vote the EU could not become a party to the Interim Agreement and terminating the provisional application of the Agreement.

The Council and Commission, faced with what they thought was an urgent need to get the agreement approved and the awkward transition to the new Lisbon Treaty procedures, had adopted the risky strategy of trying to 'bounce' the European Parliament into approving the agreement by presenting it as a *fait accompli*, an agreement already signed and about to start being provisionally applied, and which therefore could not be renegotiated. They judged that – given a choice between accepting this and rejection, with all that implied in terms of transatlantic embarrassment and security risk – the European Parliament would reluctantly, and probably with much verbal protesting, nevertheless agree. The strategy failed and as a result the legislative initiative failed too. Instead of an imperfect agreement there was no agreement.

4. THE THIRD CHAPTER: SECURITY RISKS AND FUNDAMENTAL RIGHTS

The rejection by the European Parliament provoked a storm of reaction, not least from the US.[44] Before the vote Adam Szubin, the US Treasury Department official in charge of the TFTP, said that the failure of the agreement would be 'very damaging,' stressing the amount of information given by the TFTP to EU governments, including Germany. US National Security Advisor James Jones said that EU-US data transfer had 'prevented terrorist attacks and saved lives'. Commissioner Malmström had argued in February that 'refusal of consent risks to lead to both a data protection gap and a security gap.' In April she said:

> 'This matter is very urgent. We know that there is a clear security gap since January of this year because TFTP data stored in Europe are no longer made available to the US Treasury Department, so the aim is to arrive at a signed agreement as soon as possible, preferably before the end of June.'

In fact the gap was limited, since in the absence of the agreement, specific (not bulk) transfers could be requested under the EU-US Agreement on Mutual Legal Assistance, together with the bilateral US-Member State agreements which the EU agreement supplements, and under the terms of national data protection law.[45]

The Commission and Council moved quickly to negotiate a new agreement and this time they made sure to consult the European Parliament at every turn. A draft mandate was agreed by the Commission on 24 March 2010 and agreed by Council on 11 May. The legal bases were to be Articles 87(2)(a) and 88(2) TFEU (police cooperation). The Commission made a point of stressing how much useful information was passed by the US to EU governments, citing specific examples. On 5 May 2010 the European Parliament adopted a Resolution on the Commission's draft negotiating mandate.[46] The European Parliament 'Welcome[d] the new spirit of cooperation demonstrated by the Commission and the Council and their willingness to engage with Parliament, taking into account their Treaty obligation to keep Parliament immediately and fully informed at all stages of the procedure'. The Parliament stressed the issue of bulk data transfers; these, it said, 'mark a departure from the principles underpinning EU legislation and practice' and this departure could not simply be rectified by ex post controls and monitoring. It recommended a system based on public judicial oversight based

[44] For a balanced and prescient assessment of the position after the February 2010 vote in the European Parliament, see J Monar, 'The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications' (2010) 15 *European Foreign Affairs Rev* 143.

[45] See Monar, note 44 above, at p.149.

[46] European Parliament resolution of 5 May 2010 on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the European Union and the United States of America to make available to the United States Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing P7_TA-PROV(2010)0143.

in the EU and an EU-based monitoring authority. However it also opened up the way for a compromise, suggesting a twin-track approach, based on an FMDA based on strict standards, and 'the fundamental longer-term policy decisions that the EU must address'. As far as the latter are concerned, the European Parliament argued that the best guarantee would be to carry out the extraction of data within the EU (i.e. to institute an EU TFTP); in the interim it proposed that the Commission and the Council should explore 'ways to ensure, in the meantime, that EU select personnel – from EU organs or bodies, including for example, the EDPS [European Data Protection Supervisor], or joint EU-US investigation teams – with high clearance, joins SWIFT officials in the oversight of the extraction process in the US.'

There was a US charm offensive: MEPs were invited to Washington, and US Vice-President Joseph Biden made a speech on the SWIFT agreement to the European Parliament on 6 May.

What were the key concessions, or changes, between the rejected 2009 agreement and the 2010 agreement?

- A clearer agreed definition of terrorism, based on the EU's 2002 Framework Decision.[47]
- Verification by Europol, before the data is handed over of whether the request meets the conditions in the Agreement.
- Appointment by the EU of an 'independent person' to monitor the use of data in the USA; this is intended to prevent misuse of data – data mining and industrial espionage.
- More detail on judicial redress for EU citizens as well as better regulation of rights to rectification and erasure of data.
- Regulation of onward transfer of data to third countries.

The agreement is without doubt an attempt to balance security/law enforcement objectives with data protection. Within the EU, data protection rights for individuals have a higher visibility since the coming into force of the Lisbon Treaty. Not only has Article 8 of the Charter of Fundamental Rights on the protection of personal data acquired binding force; Article 16 TFEU reiterates the right to protection of personal data and establishes a competence to enact legislation on the processing of personal data by EU institutions and agencies, by the Member States when acting within the scope of Union law, and rules relating to the free movement of such data. Nevertheless, as the Opinion on the revised FMDA by the European Data Protection Supervisor (EDPS) points out, Article 16 TFEU was not included as a legal basis for the decision concluding it, although to have done so would have served to

[47] Council Framework Decision 2002/475/JHA on combating terrorism, OJ L 164, 22.6.2002, p.3.

emphasise that the agreement is designed to protect personal data as well as to facilitate its exchange. [48] Although the EDPS recognised improvements in the new agreement, he also pointed to a number of remaining concerns:

- The EDPS was not convinced that a case had been made that the transfer of data is necessary – as opposed to useful – given existing frameworks for exchanges of data based on the mutual legal assistance agreement and arrangements between the US authorities and Europol and Eurojust. He was not convinced, he said, of the 'real added value' of this agreement.
- The EDPS was concerned that the bulk transfer of data does not meet the requirement of proportionality. The fact that the SWIFT system does not technically allow targeted searches does not per se render bulk transfers lawful.
- The EDPS argued that the maximum retention period of 5 years for non-extracted data (ie data that had not been used for any investigation) is too long.
- The negotiating mandate for the agreement had envisaged that a judicial public authority should have responsibility for receiving requests from the US Treasury and assessing compliance with the conditions for transfer. The agreement gives this task to Europol, which, as the EDPS points out, is not a 'judicial public authority'. Worse, the agreement also allows Europol to itself request information from the US: 'It is hard to reconcile this power of Europol, which may be important for the fulfilment of Europol's task and which requires good relations with the US Treasury, with the task of Europol to ensure independent oversight'.[49]
- With respect to the enforceability of data subjects' rights, the EDPS also had concerns, as a result of Article 20(1) of the agreement which provides that 'This Agreement shall not create or confer any right or benefit on any person or entity, private or public.' Given that current US privacy laws only create rights for US citizens and permanent residents, the position of EU citizens is unclear.
- The EDPS argued for the inclusion of a sunset clause as an incentive to finding a solution which would no longer require the transfer of bulk data.

The new agreement was signed on 28 June 2010. The LIBE Committee issued a Report on the new agreement on 5 July 2010, recommending consent.[50] A minority were opposed on the

[48] Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II) OJ C 355, 29.12.2010, p. 10.

[49] Opinion of the European Data Protection Supervisor, note 48 above, para 25.

[50] Recommendation on the draft Council decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the

ground that some key demands, especially relating to bulk data transfer, had not been met. The European Parliament approved the revised agreement on 8 July 2010 and it came into force on 1 August 2010.[51]

Unusually, the Council Decision concluding the agreement makes a binding commitment towards developing the EU's own equivalent to the TFTP, thus removing the need for bulk transfers of data, since the EU would be able to respond to specific requests – as the US authority now does to EU requests. However until this happens bulk transfers will still take place. Of course, different views may be taken as to whether the agreement really offers 'added value' and whether the balance between necessity and data protection is the best achievable at present. The European Parliament's change of view no doubt reflected both the improvements it identified in the new agreement, and the fact that it had this time been kept informed and involved in the negotiations throughout. It might also be argued that a Parliament with real joint legislative power acts differently from a Parliament with only the power of expressing its opinion.

European Union to the United States for the purposes of the Terrorist Finance Tracking Program, A7-0224/2010.

[51] Council Decision 2010/412/EU on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program OJ 2010 L 195/3. Both the UK and Ireland have chosen to participate in the agreement; for the UK's acceptance, see Council doc.12024/10, for Ireland's acceptance, see Council doc. 5736/11.

5. THE FUTURE: INTERNAL SECURITY WITH A GLOBAL PERSPECTIVE?

The Commission's Action Plan for the Stockholm Programme foresees the adoption in 2010 of a recommendation to authorise the opening of negotiations with the US for both an agreement on data protection for law enforcement purposes and a long-term TFTP agreement, and in 2011 of a Communication on the feasibility of a European Terrorist Finance Tracking Programme.[52] A recent Communication from the Commission on establishing a new legislative framework for data protection[53] emphasises the limitations of the existing regulation of data protection in the area of police and judicial cooperation in criminal matters,[54] and the need to review procedures and guarantees when data is transferred to third countries.

> [T]he current legal instruments include no detailed, harmonised requirements as to which transfers can be considered lawful. This leads to practices which vary from Member State to Member State. … Moreover, international agreements concluded by the EU or its Member States often require the inclusion of data protection principles and specific provisions. This may result in varying texts with inconsistent provisions and rights, and thus open to divergent interpretations.[55]

The 2008 Framework Decision on data protection in the framework of police and judicial cooperation in criminal matters, for example, leaves to the Member States the assessment of adequacy of data protection safeguards in relation to third countries to which data may be transferred.[56] In addition, Article 26 provides that

> This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements with third States existing at the time of adoption of this Framework Decision.

---

[52] The Stockholm Programme, note 2 above; Commission Communication, 'Delivering an area of freedom, security and justice: Action plan implementing the Stockholm Programme' COM (2010) 171.

[53] Commission Communication, 'A comprehensive approach on personal data protection in the European Union' 4 Nov. 2010, COM (2010) 609; see also JHA Council Conclusions on the Communication, 25 February 2011, Council doc. 5980/4/11 REV 4.

[54] The current instruments are Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60), together with Council Decision 2008/615/JHA ('Prüm Decision') on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime OJ 2008 L 210, p.1; and the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU, OJ 2000 C 197, p.1. On the fragmentation of EU regulation of data protection in relation to JHA matters, and the resulting lack of coherence and clarity in the system, see de Hert and de Schutter, note 27 above, at p.314.

[55] COM (2010) 609, note 53 above, p.15.

[56] See note 54 above.

As a result transfers made under the SWIFT agreement are subject to the safeguards contained in that agreement, not those in the Framework Decision.[57]

As we have seen, among the 'significant common threats' identified by the Internal Security Strategy approved by JHA Council in February 2010 are terrorism and serious and organised crime.[58] The European Security Model presented in this document emphasises the importance of integrating respect for fundamental rights, the rule of law and privacy into the EU's justice, freedom and security policies, and ensuring an 'effective democratic and judicial supervision' of security activities by the European Parliament, national parliaments and the European Court of Justice. The Commission's Action Plan for the implementation of the Internal Security Strategy, published on 22 November 2010, also emphasises the commitment to the protection of human rights – and indeed connects this to the inter-dependence of internal and external aspects of security:

> Internal security cannot be achieved in isolation from the rest of the world, and it is therefore important to ensure coherence and complementarity between the internal and external aspects of EU security. The values and priorities in the Internal Security Strategy, including our commitment to promoting human rights, democracy, peace and stability in our neighbourhood and beyond, are an integral component of the approach laid down in the European Security Strategy. As that Strategy recognises, relationships with our partners, in particular the United States, are of fundamental importance in the fight against serious and organized crime and terrorism.[59]

One of the actions specified under the counter-terrorism head of this Action Plan is the development of an EU-TFTP: the Commission undertakes to develop a policy for the EU to extract and analyse financial messaging data held on its own territory.

In December 2010 the Council adopted a mandate for the negotiation of an agreement between the EU and the US on personal data protection when cooperating to fight terrorism or crime.[60] This would provide the data protection regulatory context, including a supervisory mechanism, for specific agreements on data transfer, such as the SWIFT agreement, or a new PNR agreement.[61]

---

[57] See V Mitsilegas, *EU Criminal Law*, Hart Publishing 2009, at p.274.

[58] Internal Security Strategy for the European Union: Towards a European Security Model, Council doc. 5842/2/2010.

[59] Commission Communication, 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe', Com (2010) 673, p.3 (a footnote in the original text has been omitted).

[60] JHA Council Conclusions, 2-3 December 2010, Council doc. 16918/10.

[61] The same Council meeting also agreed a negotiating mandate for PNR agreements with Australia, Canada and the USA: see note 65 below. See also Commission Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM (2010) 492.

6. CONCLUDING REMARKS

So, what does the experience of the SWIFT agreement tell us about 'internal security with a global perspective', as the Commission put it in its November 2010 Action Plan?

1. The law enforcement utility of personal data held by SWIFT, an international commercial enterprise, brought it into contact with competing and potentially conflicting regulatory and security regimes. The problem was exacerbated for both US and EU law enforcement authorities by its decision to move its European data out of the US jurisdiction. For the EU, an internal data protection issue became an international security issue, requiring not only regulatory cooperation but ultimately an international agreement. Its external competence flows from this necessity: thus the intra-EU police cooperation foreseen in the Treaty is extended to third countries, such as the USA.

2. The EU is very keen to demonstrate that it is an effective actor in counter-terrorism, and an equal partner to the US. Here, it had serious difficulty over its ability to deliver what the Council and Commission had promised to the US – an agreement putting SWIFT transfers on a solid legal foundation. The irony is this: it is often claimed that the EU would be a more effective international actor if it were more supranational, more like a federal state, and less inter-governmental. Here, however, it was the increased powers of the European Parliament – that is, an increased level of supranationality – in the JHA field and in the procedure for concluding international agreements that caused the problems. By comparison, an agreement concluded under the former third pillar would not have posed these problems for the Council, which could have approved it under former Articles 24 and 38 TEU.

The history of the agreements on passenger name records with the USA and Australia is also illustrative of this point. The PNR agreement with the USA was originally concluded in 2004 under Community powers; the European Parliament bringing an action challenging the legality of the concluding decision, the Court held that Community powers could not be used to conclude an agreement the primary purpose of which was public security, combating terrorism and organised crime.[62] The Union then negotiated a new agreement with the USA which was signed in 2007 by the Council on the basis of third pillar powers, Articles 24 and 38 TEU.[63] An agreement with Australia was signed in 2008[64] and both agreements have been

[62] Joined Cases C-317/04 and C-318/04 *European Parliament v Council* [2006] ECR I-4721. See further V Mitsilegas, 'The European Union and the Globalisation of Criminal Law', (2009-2010) vol.12 *Cambridge Yearbook of European Legal Studies*, p.337 at 374-379.

[63] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of

provisionally applied since their signature (it will be recalled that provisional application was also foreseen for the first SWIFT agreement). In May 2010 the European Parliament decided to defer its consent to the conclusion of these PNR agreements with the USA and Australia and in December 2010 the Council agreed a negotiating mandate for new PNR agreements – which like the SWIFT agreement will require the Parliament's consent for their conclusion. [65]

3. The SWIFT story thus demonstrates the substantial shift brought about by the Treaty of Lisbon in the balance of power as regards international treaty-making by the EU. Wherever internal acts are to be adopted by the 'ordinary legislative procedure' (formerly known as co-decision), the Parliament must give its consent. This applies not only to agreements involving police cooperation and public security, as here, but also trade agreements. If the Parliament must give its consent to the final text, it will in practice need to be involved by the Commission and the Council at earlier stages, even though Article 218 TFEU does not give the Parliament a formal role in the adoption of the negotiating mandate or the negotiation itself. As Monar points out, although this may result in an increased democratic legitimacy, the European Parliament is not subject to the same parliamentary-majority-based disciplines as national Parliaments and the EU's executive cannot take its support for granted.[66]

Nor is the SWIFT agreement an isolated case. The Parliament's involvement in the PNR agreements has already been noted. In addition, the European Parliament has brought an action before the EU Court of Justice contesting the legal basis chosen by the Commission and Council for the revised EU Regulation on the freezing of assets of those connected with terrorism.[67] The Regulation is based on Article 215 TFEU, referring in its Preamble to the original 2002 Common Position.[68] The European Parliament is arguing that the 2009 Regulation should have been based on Article 75 TFEU (which is within the Treaty provisions

---

Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement) OJ L 204, 4.8.2007, p. 16.

[64] Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service OJ L 213, 8.8.2008, p. 47.

[65] See note 61 above. For letters to the Council from the President of the Parliament, the rapporteur and the Chair of the LIBE Committee, expressing support for the new agreements but requesting to be kept fully informed of the progress of negotiations, see Council docs.16972/10 and 17421/10.

[66] J Monar, note 44 above, at p.148.

[67] Case C-130/10 *European Parliament v Council*, action brought on 11 March 2010 (OJ 2010 C 134, p.26) challenging Council Regulation 1286/2009/EU of 22 December 2009 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban OJ 2009 L 346, p. 42.

[68] Council Common Position 2002/402/CFSPconcerning restrictive measures against Usama bin Laden, members of the Al-Qaida organisation and the Taliban and other individuals, groups, undertakings and entities associated with them OJ 2002 L 139, p.4.

on the area of freedom, security and justice and under which the ordinary legislative procedure is used) instead of Article 215 TFEU (which deals with restrictive measures against third countries, individuals and groups and under which the Parliament only has the right to be informed). The relationship between the two provisions is by no means clear[69] (demonstrating again the difficulty of separating internal and external security issues) but what is clear is the Parliament's determination to maximise its influence over counter-terrorism policy, both external and internal. The 'pillar politics' epitomised by the PNR case has not disappeared with the removal of the pillar structure by the Treaty of Lisbon.[70]

4. International counter-terrorism policy-making requires a balance between security risks and safeguarding against risks to human rights and misuse of personal data. Although the EU has developed its own internal standards and monitoring mechanisms, including the European Data Protection Supervisor, the extension to third countries of these standards and safeguards, and the ability of individuals to enforce their rights, is not always straightforward. As de Hert and de Schutter point out, 'Controlling national actors is of course much easier than controlling actors outside the legal regime of the Member State of the data subjects.'[71] The EU has in fact been accused of double standards from both directions: it has been accused of double standards in allowing data transfers to third countries, in particular the USA, without ensuring that its own internal standards are met;[72] it has also been accused of double standards by US authorities who argue that the EU institutions themselves do not necessarily abide by the standards imposed on US authorities.[73] At the heart of the problem is the fragmentation of the EU's own internal regime for handling personal data in the context of law enforcement, and its uncertain balance between the principles of availability of data (making transfers possible under certain conditions and for specific purposes), and of adequacy of data protection.

With respect to certain key partners, such as the USA, the EU has decided that an overall regulatory framework for transnational data protection is needed, and at the same time this must be compatible with its own internal standards. Here then it is not only a matter of external action being necessary to achieve internal security objectives; we can also see internal data protection objectives constraining and shaping that external action: as the Internal

[69] P van Elsuwege, 'EU External Action after the Collapse of the Pillar Structure: In search of a New Balance between Delimitation and Consistency', (2010) 47 *Common Market Law Review* 987, at pp 1009-1012.

[70] On the inter-pillar dimension of JHA and the PNR case in particular, see P Pawlak, 'The External Dimension of the Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization?' (2009) 31 *Journal of European Integration* 25.

[71] P de Hert and B de Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT', note 27 above, p.306.

[72] See further V Mitsilegas, note 57 above, at p.296.

[73] As stated by de Hert and de Schutter, note 27 above, at p.314.

Security Strategy puts it, 'Europe must consolidate a security model, based on the principles and values of the Union: respect for human rights and fundamental freedoms, the rule of law, democracy, dialogue, tolerance, transparency and solidarity.'[74]

5. The battle of assertions. There is much talk on all sides of the need to achieve an acceptable balance between security and law enforcement, and fundamental rights and data protection, between availability of data and adequacy of protection. But what is acceptable and how are the risks assessed? In practice there appear to be no objective criteria and so the debate becomes a series of assertions by different actors: the US Treasury, the EU Commission, the Council and Member States, the European Parliament. This is perhaps inevitable but it suggests that the outcome is in the end a political compromise rather than a technocratic solution. And the new EU Treaty architecture means that although the crafting of a compromise is in the hands of Commission and Council, the European Parliament will have the last word. It is perhaps too early to say whether, in reaction to the much-discussed process of securitization,[75] we will see a rebalancing and a re-politicization of Justice and Home Affairs within the EU.

6. In the case of SWIFT – as in the earlier case of PNR – EU policy appears primarily reactive: to both commercial pressure and to US requirements. There is a tendency for the EU to follow the US lead.[76] This is not the same as accepting US standards. It is unhappy sending bulk data to the US, but its response is to build its own version: an EU-TFTP which would involve EU-based authorities sifting through the bulk data, constrained by EU standards and controls. The Internal Security Strategy speaks of a European Security Model but it is not entirely clear what is specifically *European* about it. Should the EU be thinking of different and better solutions?

The EU's ambition is to be able to offer a Security Strategy that integrates internal security objectives with external instruments and policies, to use its key relationships, its neighbourhood policy[77] and partnerships to promote its internal security-related priorities. It

---

[74] Introduction to the Internal Security Strategy, Council doc. 7120/10.

[75] See for example J Monar, W Rees and V Mitsilegas (eds), *The European Union and Internal Security: Guardian of the People?* Palgrave Macmillan 2003.

[76] For a discussion of this tendency, using the EU-US PNR Agreement as an example, see J Argomaniz, 'When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms' (2009) 31 *Journal of European Integration*, 119.

[77] On the JHA and the EU's neighbourhood policy, see T Balzacq (ed), *The External Dimension of EU Justice and Home Affairs - Governance, Neighbours, Security*, Palgrave Macmillan 2009, and S Lavenex and N Wichmann 'The External Governance of EU Internal Security' (2009) 31 Journal of European Integration 83; on the JHA and EU policy towards the Western Balkans, see F Trauner, 'Deconstructing the EU's Routes of Influence in Justice and Home Affairs in the Western Balkans' (2009) 31 *Journal of European Integration*, 65.

also hopes to be able to integrate its fundamental values – including fundamental rights and the rule of law – into its policies on justice and home affairs. We have looked at only one small example of the difficulty in doing just that, especially when a third country's own security needs and different regulatory approaches come into the picture. But even this small example demonstrates the impact of an important new focus of EU external policy.

7. BIBLIOGRAPHY

Argomaniz, J, 'When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms' (2009) 31 *Journal of European Integration*, 119.

Balzacq T, (ed), *The External Dimension of EU Justice and Home Affairs - Governance, Neighbours, Security*, Palgrave Macmillan, 2009.

Cremona, M, 'Defining Competence In EU External Relations: Lessons from the Treaty Reform Process' in A Dashwood and M Maresceau (eds) *Law and Practice of EU External Relations – Salient Features of a Changing Landscape*, Cambridge University Press, 2008.

Cremona, M, J Monar and S Poli (eds), *The External Dimension of the Area of Freedom, Security and Justice*, Peter Lang-P.I.E, forthcoming 2011.

Cremona, M, 'EU External Action in the JHA Domain: A Legal Perspective' in M Cremona, J Monar and S Poli (eds) *The External Dimension of the Area of Freedom, Security and Justice*, Peter Lang-P.I.E, forthcoming 2011.

de Hert, P and B de Schutter, 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and SWIFT' in B Martenczuk and S Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations*, VUBPress, 2008.

de Kerchove, G and A Weyembergh (eds), *Securite et Justice: Enjeu de la Politique Exterieure de l'Union Europeenne*, Brussels, editions ULB, 2003.

Lavenex, S, and N Wichmann, 'The External Governance of EU Internal Security' (2009) 31 *Journal of European Integration*, 83.

Lenaerts, K, 'The Contribution of the European Court of Justice to the Area of Freedom, Security and Justice' (2010) 59 *International and Comparative Law Quarterly,* 255.

Martenczuk, B and S Van Thiel (eds), *Justice, Liberty, Security: New Challenges for EU External Relations*, VUBPress, 2008.

Mitsilegas, V, 'The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data' (2003) 8 *European Foreign Affairs Rev*, 515.

Mitsilegas, V, *EU Criminal Law*, Hart Publishing 2009.

Mitsilegas, V, 'The European Union and the Globalisation of Criminal Law', (2009-2010) vol. 12 *Cambridge Yearbook of European Legal Studies*, 337.

Monar, J, W Rees and V Mitsilegas (eds), *The European Union and Internal Security: Guardian of the People?* Palgrave Macmillan, 2003.

Monar, J, 'The EU as an international actor in the domain of justice and home affairs' (2004) 9 *European Foreign Affairs Review,* 395.

Monar, J, 'Justice and Home Affairs in the EU Constitutional Treaty. What Added Value for the Area of Freedom, Security and Justice?' (2005) 1 *European Constitutional Law Review*, 226.

Monar, J, 'The Rejection of the EU-US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications' (2010) 15 *European Foreign Affairs Review,* 143.

Papakonstantinou, V and P de Hert, 'The PNR Agreement and Transatlantic Anti-terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic' (2009) 46 *Common Market Law Review,* 885.

Pawlak, P, 'The External Dimension of the Area of Freedom, Security and Justice: Hijacker or Hostage of Cross-pillarization?' (2009) 31 *Journal of European Integration,* 25.

Trauner, F, 'Deconstructing the EU's Routes of Influence in Justice and Home Affairs in the Western Balkans' (2009) 31 *Journal of European Integration*, 65.

van Elsuwege, P, 'EU External Action after the Collapse of the Pillar Structure: In search of a New Balance between Delimitation and Consistency', (2010) 47 *Common Market Law Review,* 987.

Wolff, S, N Wichmann and G Mournier (eds), (2009) 31 *Journal of European Integration* 'Special Issue: The External Dimension of Justice and Home Affairs? A Different Security Agenda for the EU'.