(2013) 32 Yearbook of European Law 1-21

LAW AND GOVERNANCE AS CHECKS AND BALANCES IN TRANSATLANTIC SECURITY: RIGHTS, REDRESS AND REMEDIES IN EU-US PASSENGER NAME RECORDS AND THE TERRORIST FINANCE TRACKING PROGRAM

Dr. Elaine Fahey*

INTRODUCTION

Contemporary Transatlantic Relations have flourished since their formalisation in 1995 in the New Transatlantic Agenda (NTA).[1] Although not itself a binding legal Treaty, it prioritised "transatlantic security" as one of its objectives.[2] The "September 11" 2001 (9/11) terrorist attacks in the US provided a major impetus for the EU and US to engage in transatlantic security cooperation. It resulted in much legal output, specifically a wave of transatlantic Agreements in the area of Justice and Home Affairs (JHA).[3] Amongst these Agreements, two in particular were enacted so as to firstly, communicate air passenger data to the US and secondly, to legalise the exchange of personal data for the purpose of terrorist finance tracking: the EU-US Passenger Name Records (EU-US PNR) Agreements and EU-US Terrorist Financial Tracking Programme (EU-US TFTP) Agreements respectively. Over a decade after 9/11, transatlantic security cooperation is still planned in new areas, for example, cyber security and cybercrime.[4] Moreover, the success and effectiveness of transatlantic rule-making, specifically the EU-US PNR and EU-US TFTP, has inspired the EU to engage in "replica" rule-making directly related to and "inspired" by the EU-US PNR and EU-US TFTP.[5]

* **Postdoctoral Researcher, Amsterdam Centre for European Law and Governance, University of Amsterdam, The Netherlands.** E.L.Fahey@uva.nl. The author is grateful to Vigjilenza Abazi, Madalina Busuioc, Joana Mendes and Annette Schrauwen for their comments. The usual disclaimer applies.

[1] Signed in Madrid on 3 December, 1995.

[2] Other objectives included: (1) the promotion of peace, stability, democracy and development, (2) responding to global challenges, (3) world trade and (4) building bridges across the Atlantic.

[3] See Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Record Data to the United States Department of Homeland Security of 17 November 2011; COM (2011) 807 final, approved by the European Parliament in April 2012 (hereafter EU-US PNR); 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 (hereafter TFTP), OJ L 195/5. Other JHA Agreements not considered in this account include Agreements as to Europol, Extradition and Mutual Legal Assistance. See K Archick, 'EU-US Cooperation Against Terrorism' (2012) *Congressional Research Service* 7-5700 (21 May, 2012). M Cremona, 'Justice and Home Affairs in a Globalised World: Ambitions and Reality in the tale of the EU-US SWIFT Agreement', Institute for European integration Research (Working Paper No. 4/2011); M Goede, 'The SWIFT affair and the Global Politics of European Security' (2012) 50 *Journal of Common Market Studies* 214; D Curtin, 'Official Secrets and the Negotiation of International Agreements: is the EU Executive Unbound?' (2013) 50 *Common Market Law Review* 423; E Fahey, 'On the Use of Law in Transatlantic Relations: Legal Dialogues between the EU and US' *European Law Journal* (forthcoming); P. Pawlak, ed., *The EU-US security and justice agenda in action*, (EUISS Chaillot Paper, 2012); V Mitsilegas, 'EU-US Co-operation in Criminal Matters post-9/11: Extradition, Mutual Legal Assistance and the Exchange of Police Data' (2003) 8 *European Foreign Affairs Review* 515. But see 'EU-US Counterterrorism pacts at risk over snooping affair' *EUObserver.com* (5 July 2013).

[4] Council of the European Union, EU-US Summit, Joint Statement 16726/10 Presse 315, 20 November 2010, p. 3; Presidency Conclusions of the Cybercrime Conference, Budapest Conclusions (13 April 2011).

[5] For example, Proposal For a Directive on the use of Passenger Name Record data for the prevention, detection investigation and prosecution of terrorist offences and serious crime, COM(2011)32, Commission

Further still, the effectiveness of transatlantic security rule-making is lauded as a reason to warrant transatlantic rule-convergence, for example, in data protection.[6] The US Attorney General has claimed in recent times before the European Parliament that no human rights violations have *ever* resulted from transatlantic justice and home affairs cooperation.[7] By contrast, certain Members of the European Parliament have claimed that the secrecy surrounding the transmission of data under certain transatlantic Agreements makes it virtually impossible to assess their operation.[8]

In respect of the first of the two Agreements mentioned above, the EU-US PNR has its origins in US legislation passed in the wake of the 9/11 atrocities, requiring airline carriers flying into the US to provide US authorities with passenger data under threat of sanction.[9] An Agreement was eventually reached in 2004 between the EU and US requiring EU airlines flying into the US to provide US authorities with PNR data in their reservation and control systems after the departure of a flight, but controversy surrounded its impact upon fundamental rights and privacy.[10] It was struck down by the Court of Justice in 2006 and replaced by an interim Agreement in 2007.[11] The most recent EU-US PNR Agreement was concluded in 2011 and was endorsed by a majority of the European Parliament in 2012.[12] It constitutes the so-called Second Generation EU-US PNR and supersedes the 2004 and 2007 EU-US PNR Agreements.[13] It was intended to represent over a decade after 9/11, an *improved* Agreement with the US in the name of fighting serious crime and terrorism. However, it remains very similar in substance and in form to its predecessors.

As to the second Agreement mentioned above, the EU-US 'SWIFT' or TFTP Agreement[14] arose out of a scandal where the *New York Times* Newspaper published details disclosing

---

Communication, '*A European terrorist finance tracking system available options*,' COM(2011)429 final, although their precise future is far from certain. The Directive was rejected by the European Parliament in 2013: 'MEPs vote down air passenger data scheme' *EUObserver.com* (24 April 2013).

[6] 'EU urged to choose transatlantic convergence on data protection' *EurActiv* (5 December 2012). Negotiations on a transatlantic data protection framework agreement began in 2010.

[7] Attorney General Eric Holder, Remarks to the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (20 September 2011), claiming no rights violations had resulted from EU-US legal relations to date:
http://wn.com/European_Parliament_Committee_on_Civil_Liberties,_Justice_and_Home_Affairs (last access 18 January 2012).

[8] See the comments cited in 'Terrorist data oversight tainted by potential conflict of interest' *EUObserver.com* (21 December 2012).

[9] The US Aviation and Transportation Security Act of 2001.

[10] 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 (DHS), Bureau of Customs and Border Protection ([2004] OJ L 183/ 83, and corrigendum at [2005] OJ L 255/168);

[11] This specific case is discussed above; see also 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) (2007 PNR Agreement), OJ 2007 L 204/18.

[12] See above n 3.

[13] The 'Second Generation' PNR terminology is taken here from official EU documents: eg JHA External Relations Trio programme, Council doc. 12004/11.

[14] See n 3.

secret access obtained by the US to the Belgian-based Society for Worldwide Interbank Financial Telecommunications (SWIFT), a private cooperative owned, by more than 2000 organisations, routing millions of transactions each day to over 7000 financial institutions worldwide. The US Central Intelligence Agency (CIA) was revealed to be running a secret program, overseen by the US Treasury, procuring financial messaging data, for example, wire transfers, in order to track terrorist financing.[15] The US was storing all SWIFT data transfers in a "mirror" database of the EU database in the US and had subjected SWIFT through subpoenas to hand over the financial data. Thus the EU-US TFTP Agreement was ultimately entered into so as to legitimise the US program and meet data privacy concerns concerning the US extraction, use and transfer of financial messaging data without a warrant.[16] These two Agreements, EU-US PNR and EU-US TFTP, have generated much controversy concerning their retention of the data of EU citizens, their limitations on redress and their secrecy.[17]

There is no shortage of governance mechanisms or "paper trails" arising from the operation of these Agreements to date. These two Agreements or their predecessors, in the case of PNR, have been subject to many review procedures to date, pursuant to the Agreements themselves. In these procedures, the EU and the US have reviewed the Agreements jointly in EU-US PNR and EU-US TFTP, while the EU agency operating under the TFTP, Europol, has additionally engaged in self-review and has in turn been subjected to review by the Europol Joint Supervisory Body (JSB), an entity which assesses the compliance of Europol as an Area of Freedom, Security and Justice (AFSJ) Agency with EU data protection law.[18] Additionally, the Agreements provide also for *further* oversight and monitoring by various bodies and overseers.[19] However, numerous aspects of the mechanisms are shrouded in secrecy, sometimes for reasons that are not legally apparent, which impacts upon the oversight conducted and its evaluation.

These reviews and oversight arrangements have all operated outside of judicial control and thus may be described as forms of experimentalist governance, a specific theory of governance and rule-making which is increasingly applied to the EU and its AFSJ policies.[20] Experimentalist governance depicts certain rule-making in the EU to form a multi-level architecture which uses broad metrics to review this rule-making. Experimentalist

[15] 'Bank data is sifted by US in Secret to Block Terror' *The New York Times* (23 June 2006).

[16] Thereafter, the Belgian Data Protection Authority held SWIFT to be in breach of Belgian Data Protection Law and the Article 29 Working Party, the independent advisory body of the European Commission established under Article 29 of the Data Protection Directive 95/46/EC, held the transfer of data to be in breach of (then) EC data protection law: see Cremona, n 3 at 11. See also the accounts of De Goede, n 3.

[17] See Cremona, n 3; See V Pfisterer 'The Second SWIFT Agreement between the European Union and the United States of American- An overview' (2010) 11, *German Law Journal* 1173.

[18] See below, Part II, IV.

[19] See below, for example, Part II, III.

[20] See J Monar, 'Experimentalist Governance in Justice and Home Affairs' in C Sabel and J Zeitlin eds., *Experimentalist Governance in the EU* (Oxford University Press, 2010) 237 and also C Sabel and J Zeitlin, 'Learning from Difference: the New Architecture of Experimentalist Governance of the EU' in Sabel and Zeitlin eds., 1, at 2-8.

Governance generally accords much discretion to bodies, who are later subject to peer-review. Experimentalist Governance mechanisms involve many actors, including, *inter alia*, EU agencies, committees, Working Groups and horizontal or non-state actors. For example, one could say that in EU-US security Agreements, broad discretion is given to the US Treasury and the US Department of Homeland Security. Similarly, the EU and the US engage in a joint peer-review exercise, while Europol has considerable discretion in its functions under the TFTP Agreement and has limited "top-down" oversight. However, the *output* of the review mechanisms may not necessarily be explained by experimentalist governance, which offers a *structural* understanding of governance. Instead, they may also be described as "New Accountability" mechanisms, a theory which depicts instances of dispersed authority, where one looks beyond courts to seek accountability. They include seeking accountability from a range of actors in many fora, including inspectors, Ombudsmen and diverse non-judicial bodies. In EU-US PNR and TFTP, a variety of non-judicial bodies, such as inspectors and overseers, are deployed to review the Agreements.

It is argued here that an assessment of these review mechanisms to date, conducted under both Agreements and independently from the Agreements, appear to have many significant legal shortcomings. Secrecy seems to inhibit accountability and rigorous oversight predominantly. In particular, Europol, which is central to the transmission of data in the TFTP, appears not to be adequately "checked" in its functions, either under the Agreement or by processes of self-review and supervision. There is no ultimate independent adjudication authority in this process who can independently adjudicate compliance with data protection rules which is required under EU law pursuant to the caselaw of the Court of Justice,[21] rendering the process deficient. The independence of US bodies acting in an oversight capacity over EU citizens equally does not appear to be satisfactory and seems to *hamper* individuals seeking redress. These governance mechanisms have not ameliorated the substantive content of the Agreements.

Although rights and redress for citizens including rights to judicial review are explicit elements of EU-US Agreements pursuant to EU law, the national laws of the Member States law and US law, rights to redress are riddled with limitations and exclusions and are often dependent upon US law, which does not seem to protect EU citizens, adequately or equally with US citizens. Moreover, there may be difficulties in seeking judicial review of the procedures surrounding the transmission of data, given that aspects of the review procedures of the Agreement themselves are shrouded in secrecy. These difficulties seem to be borne out in emerging caselaw, which however is scant.[22]

[21] Case C-518/07 *Commission v. Germany* [2010] I-1885; see I Zemanek, 'Annotation of Case C-518/07 *Commission v. Germany*' (2012) 49 *Common Market Law Review* 1755.

[22] See T-529/09 *In't Veld v. Council*, Judgment of the General Court of 4 May 2012 [2012] ECR II-000 (under appeal: Case C-350/12), discussed below; see G Hornung and F Boehm, 'Comparative Study on the 2011 draft Agreement between the US and the EU on the use and transfer of Passenger Name Records to the US Department of Homeland Security', (14 March 2012), available at http://janalbrecht.eu/wp-

The paper assesses the remedies, redress and review mechanisms under the two Agreements since their enactment up to the present day, focussing upon the latest EU-US PNR Agreement and its evolution and the EU-US TFTP Agreement. It is argued that the operation of a plethora of governance mechanisms exposes the hollowness of review, remedies and redress within the Agreements, which do not seem to be mitigated or compensated for by rights or redress provisions, for example, to judicial review. The paper shows that there are significant shortcomings in the operation of the reviews of these two Agreements. The operation of the Agreements emphasises how law and governance mechanisms do not necessarily compensate for each other as checks and balances. Accordingly, they demonstrate reasons that the EU should be particularly cautious about replicating this rule-making in EU law, i.e. in adopting an EU PNR based upon the EU-US PNR and a TFTS, based upon the EU-US TFTP.

The rights and redress provisions and the operation of the review mechanism under EU-US PNR are considered here firstly in Part I and in relation to EU-US TFTP in Part II. The characteristics of the review mechanisms under the Agreement as governance provisions are assessed in Part III, in light of the content of rights and redress mechanism in Part I, followed by conclusions.

PART I: RIGHTS AND REDRESS UNDER EU-US PNR

I. *BACKGROUND TO THE EU-US PNR*

As outlined in the Introduction briefly, the EU-US PNR has its origins in US legislation passed in the wake of the 9/11 atrocities, requiring airline carriers to provide US authorities with passenger data under threat of sanction. The US Aviation and Transportation Security Act of 2001 required all airlines flying into the US to supply PNR data to the US Customs and Border Control (CBP), operating within the US Department of Homeland Security (DHS). Such an obligation did not appear compatible with EU law as it then was, given that Article 25 of the Data Protection Directive provided that personal information originating from within EU Member States may be transferred to a third country only if that country "ensures an adequate level of protection,"[23] a level of protection which had not formally been established between the EU and US. Thus in December 2003, the EU launched negotiations with the US on an Agreement concerning the transfer of PNR data and a draft Agreement was reached in 2004. Thereafter, undertakings as to the use of the PNR data were given by

content/uploads/2012/03/PNR-Study.pdf (last accessed 18 January 2013), noting the case of *Hasbrouck v. US Customs and Border Control*, (2010 No. 3793, United States District Court, San Francisco Division) obtaining limited procedural redress in a claim for PNR data, 17.

[23] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23 November 1995, p 31.

the US CBP, the US Agency receiving PNR data transferred.[24] The Commission meanwhile adopted an Adequacy Decision, amounting to a formal finding that, for the purposes of Article 26(5) of the Directive, the undertakings offered by the CBP provided adequate protection for the data of passengers flying to or from the United States.[25] An Agreement between the EU and US was signed between the representative of the EU Presidency and the US DHS and entered into force in 2004[26] but much disquiet remained concerning the impact of the Agreement on fundamental rights, even after the issuing of the US undertakings. As the House of Lords European Union Committee has stated, there was much uncertainty in Member State Parliaments about the legal purpose of the Agreement entered into. The Committee outlined that:

> "[the Agreement] was not intended to authorise the transfer of PNR data by the airlines to the US authorities… Its purpose was to legalise the "pulling" by CBP of PNR data … if and only if this took place in accordance with the Commission Adequacy Decision, and hence in accordance with the Undertakings ..."[27]

The European Parliament in particular continued to voice its concerns and sought in proceedings initiated before the Court of Justice the annulment both of the Commission Adequacy Decision and of the Council Decision authorising the signature of the Agreement.[28] The Court (agreeing with the Advocate General) held *inter alia* that ex Article 95 EC (now Article 114 TFEU), as the legal basis of the Council Decision read in conjunction with the Data Protection Directive, did not provide an adequate legal basis. It accordingly annulled both Decisions, and concluded that it was unnecessary to consider the Parliament's other arguments. Given the consequences of its judgment for the EU-US Agreement, the Court preserved the effect of the Adequacy Decision until 30 September 2006 to allow time for a new Agreement to be negotiated. The First Generation EU-US PNR was thus struck down by the Court of Justice solely on legal basis grounds in 2006 and not wider grounds in respect of the protection of fundamental rights. A provisional seven-year Agreement was then concluded in 2007 to replace the Agreement struck down, which De Witte notes amounted to a significantly worse legal bargain for the EU, wherein the US took advantage of the renegotiation to extend data retention periods considerably.[29] The European Parliament sought to postpone its approval vote on the 2007 Agreement,

[24] Undertakings of US CBP issued on 11 May 2004, OJ [2004] L 1235/11.
[25] Adequacy Decision of 14 May 2004. See House of Lords European Union Committee *The EU/US Passenger Name Records (PNR) Agreement* (21st Report of Session 2006-07, 5 June 2007), para 38.
[26] See above n 10.
[27] House of Lords, n 25 at para. 40.
[28] Joined Cases C-317/04 and C-318/04, *European Parliament v Council and Commission,* Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721. The Council adopted Decision 2004/496 on the basis of ex Article 95 EC in conjunction with Article 300(2) EC. Commission Decision 2004/535/EC was adopted pursuant to Directive 95/46/EC.
[29] See n 11; B De Witte, 'Too much constitutional law in the European Union's Foreign Relations?' in B De Witte and M Cremona (eds), *EU Foreign Relations Law: Constitutional Fundamentals,* (Hart Publishing, 2008), 11.

deploying its approval powers accorded to it by the Treaty of Lisbon (Article 218(6)(a) TFEU). The Parliament pressed the Commission for a global strategy on external PNR with the US, Canada and Australia which emphasised better redress and effective legal safeguards.[30] Thereafter, negotiation of a revised Agreement followed suit and a "Second Generation" Agreement was agreed in 2011. It has been described by the European Commission as an "improved" one, enhancing data protection mechanisms therein, limiting the use of data, purporting to fight crime more effectively, placing obligations on the US to share data with the EU and setting out a detailed description for the circumstances when PRN can be used.[31] Many of these specific claims as to the substance thereof are difficult to accept for reasons outlined next.

II. *CONTENT OF EU-US PNR SECOND GENERATION AGREEMENT*

The Agreement provides that carriers operating passenger flights between the EU and US must provide PNR contained in their reservation systems in the specific circumstances outlined in the Agreement. The PNR includes sensitive data, as defined in Article 6, which is "masked out" and "filtered", to be deleted after a period of 30 days. However, ordinary PNR is retained in an "active" database for five years and is "depersonalised" and "masked" for six months and may after the active period be transferred to a dormant database for up to ten years, pursuant to Article 8. The specific terms "depersonalised" and "masked" are nowhere defined in the Agreement and remain uncertain legal standards. Equally, while the 2004 Agreement limited data retention to three and a half years, the 2007 agreement permitted retention in an active database for seven years and dormant retention for eight years. Thus the Agreement represents a far-reaching one as regards individuals' rights and retention of data, despite its purported improvements, albeit an improvement on an earlier draft in 2011.[32] The PNR data may be transferred onwards to third countries pursuant to "express understandings" which purportedly incorporate data privacy protections, pursuant to Article 17, albeit that these terms appear vague, possibly unwritten, in so far as they do not seem to be required per se to be in writing under the Agreement, and even unenforceable.

The Agreement provides for a "push" system in Article 15 thereof, generally perceived as more compatible with data protection rights. A push data system is defined in Article 15 as one where airline carriers transfer PNR data *to* the DHS by secure electronic means 96 hours before a flight departure and in real time or thereafter, as specified by the DHS, thus "*pushing*" the data to the US by provision rather than the DHS extracting the data from

[30] Resulting in the *Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries*, COM(2010) 492.

[31] European Commission Press Release 'New EU-US Agreements on PNR improves data protection and fights crime and terrorism' IP/11//1368 (17 November, 2011)

[32] See Hornung and Boehm, n 22. See para. 15 of the 2004 Undertakings; Article 8 of the 2011 draft Agreement: Council doc. 10453/11 (20 May 2011).

carriers, yet providing the DHS with considerable discretion about the procedure itself. Further powers are accorded to the DHS to obtain data from carriers on a case-by case basis and also in exceptional circumstances, where there is a "specific, urgent and serious threat" to make requirements of carriers, in Article 15(5) thereof. Yet while the system is now characterised as a "push" system, the legal character of the Agreement remains significantly disposed towards US concerns and grants much discretion to the DHS to procure data in diverse circumstances. Moreover, much controversy may be said to surround the character of data transmitted. For example, Article 4(1)(b) limits the use of the data obtained under the Agreement for the pursuit of the prevention, detection, investigation and prosecution of transnational crime of a serious nature, using a five-part test.[33] This represents a significant limitation on the use of data in comparison with a previous draft of the Agreement.[34] However, its detailed and complex definition suggests that interpretation of these criteria may become significant. This appears ripe to generate inconsistent interpretations in the EU and US legal orders respectively, without any certainty in the event of conflict.

III. *REDRESS AND REMEDIES IN EU-US PNR*

The Second Generation EU-US PNR Agreement ostensibly provides for various rights of redress, subject to important limitations, exclusions and complex procedures. Thus in the EU-US PNR Agreement, rights of redress, access to personal information and rights of correction and rectification are provided in Articles 11 to 13. Article 13 expressly provides that any individual regardless of nationality, country of origin, or place of residence whose personal data and personal information has been processed and used in a manner inconsistent with this Agreement may seek effective administrative and judicial redress in accordance with US law. Moreover, it provides that any individual is entitled to seek to challenge administratively DHS decisions related to the use and processing of US law. EU citizens can petition for judicial review under an express list of US Acts in Article 13(3), including the Freedom of Information Act, the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act. However, the US Privacy Act of 1974 is not one of the listed acts and is an intentional and significant omission, limited as it is to US citizens only.[35] The agreement provides in Article 14, simply entitled "Oversight", that compliance with privacy safeguards in the Agreements will be subject to independent review and oversight by Department Privacy Officers, such as the DHS Privacy Officer, expressed to have a "proven record of autonomy" and exercise *inter alia* "effective powers of oversight,

[33] Defined as *inter alia* a crime committed in more than one country, prepared, planned directed or controlled in another country, involving an organised criminal group, with substantial effects in another country, where the offender intends to travel to another country.

[34] See Hornung and Boehm, n 22.

[35] See the unsuccessful litigation by an MEP to obtain PNR under the US FOI legislation, dismissed for "erroneously" maintaining that the airlines carriers data and the DHS data were equivalent or similar: *In't veld v. Department of Homeland Security* (2008- No. 1151, US District of Columbia District Judge Collyer) (15 December 2008).

investigation, intervention and review". In turn, the Agreement expresses itself to be subject to independent review and oversight by the DHS Office of the Inspector General, the Government Accountability Office and the US Congress. Thus considerable administrative discretion is accorded to a wide variety of US agencies who are checked in turn by further agencies and Government offices but nonetheless accorded much discretion. It does not seem that there is a truly independent adjudication authority within these provisions, arguably falling foul of the requirements of EU law.[36] However, the extent to which an EU citizen will in reality be in a position to challenge the autonomy of a US officer or the effectiveness of their powers renders such tests or standards problematic. Equally, the extent to which an EU citizen is hampered in seeking to judicially review aspects of data transmission through the sheer layers of executive oversight seems evident.

Furthermore, Article 21 provides that the Agreement does not *inter alia* create any right or benefit on any person. In this regard, a leaked self-expressed "non-paper" disclosed notable differences in 2011 between the EU and US as regards the negotiation of the EU-US PNR, one of which was that the Agreement would not create any new rights under US law.[37] The necessity for such a provision seems curious as it purports to empty the redress provisions of the Agreement of benefits or discourages judicial interpretation in favour of conferring legal entitlements upon litigants, arguably the antithesis of redress. These represent complex formulations of rights and remedies, riddled with limitations and shortcomings.

IV. *REVIEW MECHANISMS OF EU-US PNR*

The Second Generation EU -US PNR Agreement is subject to a joint EU and US Review process, detailed in Article 23. It provided thus that a review was to take place one year after the entry into force of the Agreement and that a review should take place regularly thereafter, as well as for an evaluation four years after its entry into force.[38] The EU is represented in the review procedure by the Commission, while the US is represented by the Department of Homeland Security, and the procedure includes experts on data protection and law enforcement and requires security clearance for participation as well as confidentiality. The US DHS is under an obligation to provide data and is expressly permitted to respond to the review report with written comments. The Second Generation Agreement has not yet been reviewed but earlier reviews of the First Generation Agreement are worthy of consideration.

In the first joint PNR EU-US First Generation Agreement review in 2005, a year after its entry into force, a review was conducted by the EU of the undertakings given by the US and a

[36] See Case C-518/07, *Commission v. Germany*, n 21.
[37] See EU-US data protection negotiations during 2011, Council doc. 5999/12, Annex note from Commission DG Justice.
[38] See the additional Declarations in the Annex.

redacted version was later published, thereby limiting assessment thereof.[39] The overall conclusion reached by the review was that substantial compliance had occurred with the conditions set out in the undertakings. This conclusion was reached despite significant criticisms being levied by the EU team that the US team had *limited* the records which could have been accessed by the EU team.[40] Breaches of individuals' rights were identified by the review as having occurred in a particular period during which the US Customs and Borders Protection (CBP) was not able to discern whether it had received data requests as to EU-US PNR on account of failures in its systems. In some instances, the US was adjudged by the EU to have exceeded the requirements of its undertakings. However, in the review of the provisional agreement adopted in 2007 which took place in 2010,[41] the EU team concluded that satisfactory information had been provided by the US to prove that the PNR served its purpose of fighting terrorism. The EU team held that the DHS had generally implemented its commitments towards the EU, finding that the provisions permitting the sharing of data with third countries had been strictly interpreted. The EU expressed its concerns about disproportionate uses of PNR and *ad hoc* non-systematic requests but nonetheless reached conclusions finding the operation of the Agreement to be satisfactory. Equally, despite the fact that the implementation of the "push" method was found not to have been technically correct, the EU team was accommodating to these issues in its overall review. On balance, these procedures seem to fall short of robust review and have operated to accommodate non-compliance with data protection requirements. Whether substantively different conclusions under the latest Agreement will emerge remains to be seen.

PART II: RIGHTS AND REMEDIES UNDER EU-US TFTP

I. *BACKGROUND TO THE EU-US TFTP*

The specific background to the development of an EU-US TFTP Agreement has been outlined in the Introduction. It suffices to recall that the objections on the part of *inter alia* the European Parliament and the Article 29 Working Group[42] to possible infringements of rights arising from US access to data held by the Belgium-based SWIFT cooperative prompted the subsequent adoption of the EU-US TFTP Agreement. As Cremona states, the origins of the Agreement in EU law were in the form of "soft law".[43] Thus soft law "Representations" were undertaken by the US thereafter as to the use by the US of the EU

[39] Commission Staff Working Paper of the Joint Review of the implementation by the US Bureau of Customs and Border Protection of the Undertakings set out in the Commission Decision 2004/535/EC of 14 May 2004, COM(2005) final (12 December 2005), not paginated.
[40] Article 23 of the latest Agreement ameliorates this information requirement.
[41] Report on the joint review of the implementation of the Agreement between the EU and US on the processing and transfer of Passenger Name Record data by air carriers to the US Department of Homeland Security, 8-9 February 2010 (Brussels, 2010).
[42] See n 16 above.
[43] Ibid, 12.

data from SWIFT. They were subsequently published in the Official Journal in 2006 in the form of a letter from the US Department of Treasury, stating that:

> ".. TFTP contains multiple, overlapping layers of governmental and independent controls to ensure that the data, which are limited in nature, are used strictly for counterterrorism purposes …."[44]

They established a basis for the TFTP in US law and not EU law and were predicated upon the involvement of SWIFT with the US Treasury. These Representations were followed by the agreement of the US to the appointment of an ''Eminent European Person" to review *inter alia* the use of the data, who produced two reports in 2008 and 2010, classified as secret, which were distributed to the permanent representatives of the Member States, to outline how *effective* TFTP had been in the aftermath of certain significant terrorist attacks and confirmed US compliance with the Representations.[45] The review conducted was thus not transparent as to its methodology. A formal Agreement between the EU and US became necessary when in 2010, SWIFT altered its systems and all data concerning EU internal transactions began to be held at two European sites, entailing it would no longer be "mirrored" in the US.[46] An EU-US TFTP Agreement finally reached in 2009 was vetoed by the European Parliament in 2010, again exercising its powers of approval accorded by the Treaty of Lisbon, pursuant to Article 218 TFEU.[47] Judicial remedies and fears of bulk transfers were reported to be the basis of the concerns warranting the rejection of the Agreement.[48] A second SWIFT agreement was reached in 2010 and entered into force also in 2010. The legal basis of that Agreement is in Articles 87(2)(a) and 88(2) TFEU,[49] the former providing for competence in police cooperation in the area of the collection, storage, processing, analysis and exchange of relevant information and the latter, to regulate the tasks and operation of Europol. Also, the new provision of the Treaty of Lisbon protecting the privacy of the personal data of EU citizens, Article 16 TFEU, is explicitly invoked in a recital to the Agreement, presumably to enhance its apparent commitment to respecting fundamental rights in the Agreement. A request by an MEP to disclose a classified Council Service Legal Opinion suggesting the *earlier* legal basis of the Agreement was flawed,[50] succeeded in part

[44] [2007] C 166/08, mentioned in Recital 8 to the later Agreement.

[45] See J-L Bruguiere 'Second report on the processing of EU-originating personal data by the United States Treasury Department for Counter Terrorism Purposes: Terrorist Finance Tracking programme' (2010), available at http://www.statewatch.org/news/2010/aug/eu-usa-swift-2nd-bruguiere-report.pdf (last accessed 18 January 2013).

[46] And also in the absence of an EU version of the TFTP Agreement for the EU.

[47] See A Ripoll Servent, & A MacKenzie, 'The European Parliament as norm-taker? EU-US relations after the SWIFT Agreement' (2012) 17(5) *European Foreign Affairs Review* 71.

[48] 'MEPS hail Historic rejection of SWIFT deal,' *Agence Europe* 13 February 2010.

[49] In conjunction with Article 218(5) TFEU, providing the Council with competence to enter the Agreement.

[50] Which was Articles 82(1)(d) and 87(2)(a) TFEU, the former providing competence for judicial cooperation between the States in criminal matters.

before the General Court recently and is pending on appeal, indicating again the operation of secrecy in diverse levels.[51]

II. *CONTENT OF THE EU-US TFTP*

The EU-US TFTP Agreement provides in Article 1 that its purpose is to prevent, investigate, detect and prosecute terrorist financing, by providing to the US Treasury exclusively data stored in the territory of the EU. There are many novelties arising from these legal objectives, granting exclusive authorisation to a sovereign agent of US Government.[52] The TFTP Agreement is expressed in Recital 2 thereof to have been instrumental in capturing and in generating "leads" that could be disseminated as counter-terrorism information around the world. This formula of "leads" or a "nexus" to terrorism is the basis of operation of the Agreement, despite its vagueness or lack of clarity.

The purpose of the Agreement as set out in Article 1 above indicates that it is a joint cooperation between the EU and US but is predominated by content and provisions granting access to obtain financial messaging data by granting extensive legal powers to the US Treasury.[53] Europol has a vital role under the Agreement and operates as the Designated Provider pursuant to Article 4. It is served with requests from the US Treasury for data which it must consider pursuant to Article 4(2) as to whether it is identified as clearly as possible, that its necessity is substantiated and that the request is tailored as narrowly as possible to minimise the amount of data sought. Europol thus possesses considerable discretion. This process operates in secret as the requests are classified by Europol. At this point of verification by Europol, the US request is expressed to have "binding legal effect as provided under US law, within the European Union as well as the United States," and at this point Europol provides the data on a "push basis" directly to the US Treasury**.** Such a standard of "binding legal effect" appears to be expressed so as to enhance its certainty and its compliance with the rule of law. Nonetheless, the expression of the legal effects of the request for data by the US seems to be predicated upon mutual recognition or legal equivalence between legal orders. Such a formula is not substantively part of the Agreement, which instead appears more imbalanced in respect of the redress and remedies accorded to EU and US citizens respectively. Arguably, this provision serves to emphasise the complex character of *other* redress and remedies provisions in the Agreement, explored here next.[54]

III. *RIGHTS AND REDRESS UNDER EU-US TFTP*

[51] See T-529/09 *In't Veld v. Council* where the General Court held *inter alia* that a Legal Service Opinion of the Council in transatlantic relations was a document which did not warrant secrecy classifications in the public interest.

[52] Cremona, n 3.

[53] See Pfisterer, n 17.

[54] A limited *converse* legal power for the EU (so-called reciprocity) is provided for in Article 10, enabling EU requests emanating from a Member State law enforcement body or EU agencies, for example, Europol so as to obtain information arising from a search of TFTP, highlighting the nature of the Agreement.

Similar to the EU-US PNR Agreement, rights of access to the data transmitted under the Agreement or rights to ascertain whether data has been transmitted in breach of the Agreement and rights to seek rectification, erasure and blocking are provided for in Articles 15 and 16 respectively. However, Article 15(2) heavily qualifies the former and provides for a broad array of limitations, stating that disclosure to an individual of his personal data processed under the Agreement may be subject to reasonable legal limitations applicable under law to safeguard the prevention, detention, investigation or prosecution of criminal offences, and to protect public or national security with due regard for the legitimate interests of the individual. This provision operates by way of a defence and represents a highly circumscribed limitation or hollowing of the rights of a litigant.

Where an individual asserts that their data has been processed in breach of the Agreement, an ostensibly broad right to seek effective administration and judicial redress under EU law, the national law of the Member States and US law is provided for in Article 18, stated to exist irrespective of nationality or country of origin. There is in particular, "a process" to seek judicial review under US law arising from adverse administrative action. The question remains as to the reality or real content of this redress for the following reason. Recital 12 of the Agreement provides that administrative and judicial redress is available under US law for the mishandling of personal data pursuant to a list of laws, stated to include the Administrative Procedure Act of 1946, the Inspector General Act of 1978, the Implementing Recommendations of the 9/11 Commission Act of 2007, the Computer Fraud and Abuse Act and the Freedom of Information Act. By an overtly intentional omission, EU citizens qua litigants are excluded from litigating the US Privacy Act 1974, similar to the EU-US PNR Agreement, representing a significant exclusion from substantive US law and an unequal application of remedies between the legal orders. As a result, EU citizens are deprived of specific legal redress for unwarranted uses of personal information by federal agencies, otherwise available to US citizens.

A more procedural rather than substantive complaint to the operation of redress under the Agreement might be the following. Pursuant to Article 16 of the Agreement, an EU citizen seeking rectification, erasure or blocking must complain to their national supervisory authority, who in turn transmits the request to the Privacy Officer of the US Treasury. As in the EU-US PNR Agreement, there are thus considerable layers of administrative control across jurisdictions that an individual litigant must surmount in order to allege a breach of their rights, layers where much discretion is vested therein. A similar objection might be made to other safeguards within the Agreement. Whereas the PNR Agreement refers to "Oversight" in Article 14 thereof, the TFTP Agreement outlines provision for "monitoring of safeguards and controls" in Article 12, by way of oversight from so-called "independent overseers," including a person appointed by the European Commission with agreement and security clearance from the US, expressed to be subject to regular monitoring, including of its independence. This oversight is subject to monitoring by the Inspector General of the US

Treasury. Considerable powers are accorded to these overseers in Article 12, for real time and retrospective analysis of data and powers to block data which is adjudged to be neither necessary nor proportionate, pursuant to the Article 5. An interim EU overseer to be based in the US Treasury was appointed in August 2010 and their identity was not disclosed.[55] A permanent unnamed EU overseer was appointed in 2012 as well as a deputy overseer, their undisclosed identities constituting a further layer of secrecy, the legal reasons for which remain unclear.[56] These oversight reports have not been publicly disseminated and ostensibly appear to be classified as secret, although this is not explicit in the text of the Agreement.

Article 17 provides for an obligation to maintain accuracy of information transmitted or received under the Agreement, entailing that appropriate measures must be taken to prevent and discontinue erroneous reliance on inaccurate data. The US Treasury remains under an obligation of transparency, to provide information to the data subjects of the TFTP through its website, pursuant to Article 14 of the Agreement. Where data is erroneously transmitted or erased or blocked, redress is provided for pursuant to the Agreement explicitly in Article 18, whereby the US Treasury and Member State must act promptly to inform and consult each other in the event of data being processed in breach of the Agreement. Overall, these provisions are substantively similar to the EU-US PNR Agreement. Significant powers and discretion are thus vested in the US Treasury by way of oversight. A final independent adjudication authority is absent from this decision-making rubric. There are notably less explicit constraints on the US Treasury under EU-US TFTP than under EU-US PNR in terms of further oversight, which does not make a favourable contrast.

IV. *REVIEW MECHANISMS OF EU-US TFTP*

Article 13 of the TFTP provides for joint review of the safeguards, controls and reciprocity provisions of the Agreement on a regular basis with the possibility for additional reviews. The review is required to consider the number of financial payment messages accessed and "leads" that have been "shared".[57] In the Review, the EU is represented by the Commission and the US by the US Treasury. The Review includes experts in security and data and a person with judicial experience and members of two national data supervisory authorities. In 2011, six months into the entry into force of the TFTP Agreement, such a 'joint review' was conducted of TFTP by teams of EU and US officials.[58] Notably, one member of the EU

[55] See the request by a European Parliament Question to reveal the name of the interim overseer appointed in August 2010, which was refused: Question of 17 October 2010 (E-8327/2010).

[56] A deputy EU overseer has also been appointed, as revealed in the second joint review between the EU and US of the implementation of the TFTP Agreement, SWD(2012) 454 final (October 2012), para. 2.1.3, considered in Part IV, next.

[57] Pursuant to Article 13(2) of the Agreement.

[58] Commission Report on the joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the

'review' delegation was excluded from the review after having been denied security clearance by the US, upsetting the ostensibly joint nature of the review, albeit that *US-provided* clearance is a condition of the review procedure.[59] One specific recommendation made by the review was that more statistical information should be made available in future reviews conducted of the Agreement. It concluded that it was difficult to assess the concrete value of information from TFTP and that the effectiveness of the Agreement would have to be considered over a much longer period. A second joint review published in late 2012 reviewing a longer time period than the first review, made few substantive recommendations.[60] Some information was only provided to the EU reviewers on the condition that it was treated as EU Secret and team members had to sign non-disclosure agreements in addition to obtaining clearance, conditions which were accepted by the EU as necessary despite their impact upon the oversight. The second review found that the US was conducting less actual searches of the data but that the overall amount of data transferred was still not being disclosed to the EU and the EU was not critical of this non-disclosure. The review notably held that the discretion accorded to Europol in its verification function made it difficult to check its final judgments. The report is striking in its tone, seeking further transparency but seemingly acquiescent to shortcomings in information and the unchecked discretion of Europol.

A self-review process conducted by Europol of its role as to TFTP was published in 2011.[61] Europol concluded in April 2011 that it was discharging its responsibilities with great care and that it had strictly followed the interpretation of the Agreement, 'as clarified by the European Commission and US'. [62] This review process by Europol itself was in turn to be subjected to another review body, this time the Europol Joint Supervisory Body (JSB). The operations of Europol are subject to supervision by the Europol JSB. The main functions of the Europol JSB involve examining proposals from Europol to exchange personal data, ensuring that the rights of individuals are not violated.[63] Crucially, however, it has no power to block disproportionate or unnecessary data transfers, despite its mandate to protect fundamental rights. The Europol JSB reported in 2011 that overall certain data protection

European Union to the United States for the purpose of the terrorist finance tracking program, 17-18 February 2011 (Brussels, 2011).

[59] Ibid, at 3.

[60] See n 56.

[61] See 'Europol Activities In Relation To The TFTP Agreement Information- Note to the European Parliament', (Brussels 14 March, 2012), http://europoljsb.consilium.europa.eu/media/205081/tftp%20public%20statement%20-%20final%20-%20march%202012.pdf (last accessed 18 January 2013).

[62] Ibid.

[63] See the outline of its function in the Introduction above. See also Article 34 Europol Decision: 'An independent Joint Supervisory Body shall be set up to review, in accordance with this Decision, the activities of Europol in *order to ensure that the rights of the individual are not violated*…'Council Decision of 6 April 2009 establishing the European Police Office (Europol) [2009] OJ L 121/37 and its public website: http://europoljsb.consilium.europa.eu/about.aspx.

requirements were not being met in the operation of the TFTP Agreement and that the requests received by Europol from the US were not specific enough to decide whether to approve them or not.[64] The Second Inspection Report of the Europol JSB was published in 2012 and is remarkably brief.[65] Of note is that the Report was "self-classified" by the Europol JSB as secret, who sought to rely upon Europol's classification of TFTP data as *EU Secret* rather than specific legal provision relating to its own powers. [66] Despite determining "progress" to have taken place as regards the operation of the Agreement, the Second Report found numerous operational shortcomings, rights infringements and outlined a lack of transparency in the operation of the Agreement. Also, it found most significantly that Europol had *never* refused US requests. The Report recommended that requests from the US had to better "substantiated", given the amount of "non-suspect" data being transferred. Moreover, the JSB outlined what it termed were the *challenges* for Europol of attempting to limit the data provided, data which it explained was presently provided for a time frame containing *every single day of the year*, drawing conclusions which fell short of a robust critique of the role in Europol in permitting daily transfers of data.[67] This report prompted the European Parliament to table a question to the European Commission as to whether Article 4 of the Agreement could be considered implemented if all data was being transferred to the US, suggesting that the conclusions of the report were "alarming".[68] In 2013, the Europol JSB assessed the implementation of its previous recommendations.[69] While the Europol JSB found that the Department of Treasury had substantially improved the "content, relevancy, accuracy, accountability and readability" of Article 4 requests, nonetheless the phenomenon of "massive and regular" transfers to the US remained unchanged, arguably drawing unconvincing conclusions given its mandate to protect fundamental rights. Whilst it admitted that there was an inevitable tension between limiting the amount of data sought and transmitted, it suggested that these were essentially "*political*" issues for legislators to determine. From this we can discern that the Europol JSB is renouncing any further intensity in the standard of review that it exercises under the Agreement.

[64] Report on the inspection of Europol's Implementation of the TFTP Agreement, conducted in November 2010 by the Europol Joint Supervisory Body, Report No. JSB/Ins. 11-07 (Brussels, 2011).

[65] Europol JSB Press Statement, 'Europol JSB inspects for the second year the implementation of the TFTP Agreement' Brussels (14 March 2012). The report is four pages in length.

[66] For an explanation of the secrecy classification of documents system operated in the EU, see Curtin above, n 3, 427-430.

[67] Recently, a conflict of interest was asserted to exist on account of the overlap of membership of the European Commission TFTP Review team and the Europol JSB, which parliamentarians allege has undermined the independence of the review process: See, 'Terrorist data oversight tainted by potential conflict of interest', n 8.

[68] Question tabled of behalf of the ALDE group of 25 June 2012 on the Implementation of the EU-US TFTP Agreement. The present author has been unable to find the terms of a reply to this question.

[69] 'Implementation of the TFTP Agreement: assessment of the follow-up of the JSB recommendations' Ref. 13-01 (Brussels, 18 March 2013).

Shortcomings in the reviews of the TFTP Agreement seem to be directly attributed to Europol itself, on account of its classification of TFTP as *EU secret* and its broad discretion to verify requests, which in turn impact upon its oversight. The legal evolution of Europol is the subject of much pending and proposed reforms. It remains a *fledgling* EU agency which has limited parliamentary and judicial oversight.[70] As a result of its status, there is no single legal framework in place for the European Parliament to access the workings of Europol in TFTP. For example, the main access to documents legislation in the EU, Council Regulation 1049/2001,[71] does not yet apply to documents held by Europol. Similarly, pursuant to Article 263 TFEU, the Court of Justice has been granted jurisdiction to review the acts of Europol, after the expiry of a five year transitional period after the entry into force of the Treaty of Lisbon.[72] As such, judicial scrutiny of Europol is not yet possible.[73] There are thus considerable legal and political limitations in holding Europol to account. These limitations show how shortcomings in the review procedures of the TFTP Agreement are not easily remedied or likely to be amended in the immediate future.

The next section considers the nature of the review mechanism and how they related to the legal remedies in the Agreements.

PART II: GOVERNANCE MECHANISMS WITHIN TRANSATLANTIC SECURITY RULE-MAKING: ASSESSING THE RELATIONSHIP BETWEEN RIGHTS, REDRESS AND REVIEW

As outlined above in the Introduction, experimentalist governance is a theory of governance which depicts certain rule-making in the EU to constitute a multi-level architecture which often requires broad review processes. The review mechanisms of Transatlantic security Agreements are suggested here to constitute forms of experimentalist governance, operating outside of judicial controls, within a framework of rules between the EU and US, agencies and their review bodies. Within the Area of Freedom, Security and Justice (AFSJ), the domain of transatlantic relations, experimentalist governance is asserted by Monar to have a broad application, from the macro-political level right down to micro-legal instruments. For example, it forms a distinct aspect of the major policy document of the EU

[70] Europol was established by an International Convention in 1995 and became an EU Agency in 2009. A Proposal for a Regulation on Europol looks set to be adopted in 2013, envisaged in Article 88 TFEU: Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final. See M Busuioc, D Curtin and M Groenleer, 'Agency growth between autonomy and accountability: the European Police Office as a 'living institution' (2011) 18(6) *Journal of European Public Policy* 848.

[71] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [2001] OJ L 145/43.

[72] Article 10, Protocol No. 36 Transnational Provisions.

[73] Although a decision under appeal to the Court of Justice may have some impact upon the analysis here, ie there are clear legal pressures to expand the transparency of EU international relations: see T-529/09 *In't Veld* n 22.

institutions in the AFSJ, the Stockholm Programme.[74] Characteristics of experimentalist governance include mechanisms which are "non-standard" within EU law, deploy "soft law" adjudication tools, for example, that are non-binding or unenforceable, involve "learning experiences" and /or operate outside of judicial controls. Example of these are to be found in most review mechanisms of Transatlantic Agreements, including "Eminent persons" acting as independent reviewers,[75] mandatory Agreement review mechanisms, i.e. of the worthiness of prolonging the Agreement,[76] periodic joint reviews, programmed targeting, "sunset clauses"[77] and external expert reviewers.[78] Experimentalist governance would suggest that these review procedures have become "learning spaces," where knowledge is generated. However, much depends upon the character of knowledge generated and how it is implemented in the specific review processes.[79] While some caution against the impact of transatlantic security measures on individual rights under EU law and the US dominant agenda in this field,[80] others have argued that US cooperation with the EU in Justice and Home affairs has operated to *raise* US standards of data privacy.[81] In this regard, while information or knowledge functions as a form of "soft law" governance in transatlantic security, it may not have a similar output or effect in both legal orders equally.

Experimentalist governance possibly offers a *structural* understanding of transatlantic security rule-making but offers less of an understanding about the type of *output* from this rule-making. The nature of the accountability mechanisms provided for in transatlantic JHA agreements may also be described as "New Accountability" mechanisms.[82] "New Accountability" depicts instances of dispersed authority, where one looks beyond courts to seek accountability. "New accountability" mechanisms are diagonal and horizontal structures. They include seeking accountability in a broad range of forums, individuals, inspectors, Ombudsmen and offices, not fitting within the traditional top-down principal-agent relationship of governance. In transatlantic security, authority is dispersed or distributed between the EU and US, as well as various agencies and offices and considerable

[74] J Monar, 'Experimentalist Governance in Justice and Home Affairs', see n 20.
[75] As expressly initially in the TFTP Representations.
[76] Eg 5 year review, EU-US Extradition Agreement [2003] OJ L 181/27, Article 21*;* 5 year review: EU–US Agreement on Mutual Legal Assistance [2003] OJ L 181/34, Article 17. Similar mechanisms can be found in the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service [2012] OJ L 186/4: 4 year review, Article 24
[77] 5 year duration: TFTP Agreement, Article 23; 7 year duration EU-US PNR Article 26.
[78] For example, Article 13(3) TFTP; Article 23(2) EU-US PNR.
[79] Drawing here from the characteristics set out by Monar, above n 20.
[80] See Cremona, n 3.
[81] See G Shaffer 'Globalisation and social protection: the impact of EU and international rules in the ratcheting up of US data privacy standards' (2000) 25 *Yale Journal of International Law* 1; A Bradford 'The Brussels Effect' (2012-2013) 107 *Northwestern University Law Review* 1 ; Fahey, n 3.
[82] M Bovens, 'New forms of Accountability and EU-Governance' (2007) 5 *Comparative European Politics* 104; See also A Arnull and D Wincott, *Accountability and Legitimacy in the European Union* (Oxford University Press, 2003); C Harlow, *Accountability in the European Union* (Oxford University Press, 2002); D Curtin, P Mair, Y Pappadopoulous eds., *Accountability and Governance* (Routledge, 2011).

discretionary powers are accorded to the latter. Equally, the legal goals of the transatlantic Agreements, especially TFTP, are explicitly orientated towards US objectives on EU territory, suggesting some dispersal of authority. The Agreements seem to contain many non-standard accountability mechanisms in the form of "New Accountability" mechanisms. For example, the "Eminent Person" review or EU overseer reviews constitutes the use of distinctive actors. EU-US Joint Reviews operate in a broad forum, using many information sources[83] and diverse settings, with the EU and US acting horizontally as peers. "Learning from experience" is also a characteristic of "New Accountability", i.e knowledge is generated from the review processes, which will in turn ameliorate the process itself. As a result, "New Accountability" diverges from the traditional conception of law, which is predicated upon unitary authority and places courts at the pinnacle of accountability structures. In this more traditional framework, courts adjudicate upon the basis of existing knowledge.[84] By contrast, while the "New Accountability" mechanisms of Transatlantic Security Agreements generate information, as this account has demonstrated, these mechanisms have tolerated less than full disclosure of information or shortcomings in the provision of information. While experimentalist governance or "New Accountability" may provide ways to *explain* Transatlantic Agreements, they are lenient theories concerning inadequacies and instead seek to impose improvements in processes. However, as the account here outlines, review mechanisms may not necessarily compensate for shortcomings. The desire to employ such governance or "New Accountability" still has to be balanced with the need for traditional mechanisms so as to enable individuals to realise their rights.[85] Traditional mechanisms in this context would appear to be the legal remedy of litigation qua judicial review.

Challenging "oversight" controls in EU-US PNR appears to entail that an EU citizen is seriously hampered in seeking judicial review through complex layers of oversight. The latest EU-US PNR Agreement is explicitly predicated on the basis that no new rights are created there. EU citizens are excluded from alleging privacy violations under US law, despite vague provisions in the EU-US PNR Agreement on onwards transfer of data. The TFTP subjects rights to broad State-oriented exceptions. Furthermore, the TFTP masks the EU oversight of the Agreement for reasons that are not explicit or transparent.

Thus while rights to litigate or a right of judicial review is explicitly enshrined in the Agreements, it seems hampered by the general formulation of rights and redress in the Agreements, by the operation of secrecy in the Agreements and by the cumulative inadequacy of the review processes which have not substantively improved the Agreements. Moreover, limited caselaw in this area may be indicative of the practical or procedural difficulties that litigants face in challenging the operation of transatlantic

[83] The Second TFTP review involved database demonstrations, overseers, experts, data review and a broad range of specific expertise.
[84] See J Scott and D Trubek, 'Mind the gap: law and new approaches to governance in the European Union' (2002) 8 *European Law Journal* 1.
[85] See Bovens, n 82.

security. The question remains then as to what courts can review. The TFTP Agreement provides explicitly for secrecy and security as broad defences in Article 15 thereof. National security may also operate as a powerful defence in many jurisdictions. Ultimately, the Agreements appear irreparably imbalanced and are predicated upon exceptional legal circumstances, transferring vast quantities of data to the US for its benefit. Striking any meaningful balance in this situation seems challenging. Permitting secrecy and highly layered controls to co-exist, which are themselves riddled with limitations, is not a recipe for adequate checks and balances.

CONCLUSION

There is no shortage of governance mechanisms in the two Agreements considered here. Nor is there a dearth of express rights or remedies in the Agreements. The shortcomings of governance and accountability mechanisms in transatlantic security are attributable in part to secrecy classifications shrouding review, as well as a lack of independent scrutiny and peculiar legal objectives disposed towards one party. There are considerable legal challenges in assessing the effectiveness of security agreements shrouded in part by secrecy. Innovative uses of law and governance may form a characteristic of contemporary transatlantic relations, but as this account has demonstrated, this may not necessarily always be for the benefit of citizens. The operation of the Agreements thus far demonstrates the obstacles impeding the achievement of appropriate checks and balances in transatlantic security. In the case of EU-US PNR and TFTP, governance and law do not necessarily compensate for each other as checks and balances, operating instead as a worrisome legacy of post 9/11 legal developments in transatlantic relations.