UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

Maria Tzanou, 'The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?' (2015) 31(80) Utrecht Journal of International and European Law 87, DOI: http://dx.doi.org/10.5334/ujiel.cq

RESEARCH ARTICLE

The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?

Maria Tzanou[1]

[1] Keele University, United Kingdom
m.tzanou@keele.ac.uk

The EU-US Passenger Name Record (PNR) agreement has been among the most controversial instruments in the fight against terrorism that the EU negotiated with the US after the 9/11 terrorist attacks. The agreement has been heavily criticised for its implications regarding fundamental rights, in particular the rights to privacy and data protection. Nevertheless, the EU has put forward plans to develop its own PNR programme. The present article aims to examine the new dynamics concerning privacy that arise from the transatlantic fight against terrorism. It argues that, while attempts for the development of a transatlantic privacy protection framework have been made, 'spillovers' of security, taking the form of internalisation of external counter-terrorism measures, are prevalent in the era of the war against terror.

Keywords: privacy; data protection; counter-terrorism; PNR

Introduction

The European Union (EU)- United States (US) Passenger Name Record (PNR) agreement has been among the most controversial instruments in the fight against terrorism that the EU negotiated with the US after the 9/11 terrorist attacks. The agreement has been heavily criticised for its implications regarding fundamental rights, in particular the rights to privacy and data protection. More recently, revelations that the United States' National Security Agency (NSA) has been operating a secret mass electronic surveillance programme – including the collection of vast amounts of data about the time, duration and location of telecommunications[1] – sparked a heated debate in Europe about the threats to privacy in the digital era. The European Union was especially critical of the secret activities of the NSA, and the European Parliament Civil Liberties (LIBE) Committee, in its January 2014 report on the NSA surveillance programme and its impact on EU citizens' fundamental rights,[2] condemned the NSA's systematic, blanket collection of personal data and voiced its concerns, among others, as to 'the high risk of violation of EU legal standards, fundamental rights and data protection standards.'[3]

Nevertheless, the EU has put forward its plans to develop its own PNR programme that is markedly similar to the EU-US PNR agreement. Furthermore, the EU Commissioner of Justice, Viviane Reding, has responded to the disclosures about the NSA surveillance by proposing the adoption of an agreement on stronger secret

[1] They are also collecting Internet data, such as email, chat, videos, photos and file transfers held by leading Internet companies. *See* articles in the Glenn Greenwald and Ewen MacAskill 'NSA Prism program taps in to user data of Apple, Goodle and others' *The Guardian* (7 June 2013), <www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data> and the Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program' *Washington Post* (7 June 2013), <www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet- companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>.

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

[3] Ibid.

service cooperation among the EU Member States that would ultimately culminate in the creation of a European Intelligence Service to counteract the NSA.[4]

The present article aims to examine the new dynamics concerning privacy that arise from the transatlantic fight against terrorism. It argues that, while attempts have been made for the development of a transatlantic privacy protection framework, 'spillovers' of security taking the form of internalisation of external counter-terrorism measures are prevalent in the era of the war against terror. In this respect, using the PNR case as an example, the article submits that a fundamental paradox in the EU's fight against terrorism is emerging: external security measures severely criticised by the EU institutions for violating EU privacy and data protection standards are followed by proposals for the internalisation of the same or similar internal security measures which call into question the common vision of the EU as the cradle of privacy protections.

This article is structured as follows. First, it presents a brief overview of the EU-US PNR saga. It then addresses the contention articulated by James Whitman that Europe and the US are 'two western cultures of privacy' by taking a look at the EU and the US privacy regimes. Subsequently, it discusses the need for the development of a transatlantic privacy and data protection framework and critically examines the relevant existing proposals. Finally, it investigates the EU's own PNR proposal and argues that 'spillovers' of security are taking the front seat to potential 'spillovers' of privacy in the transatlantic fight against terrorism.

1. An overview of the EU-US PNR programme

The EU-US PNR saga is a story fraught with a plethora of conflicts: security versus privacy;[5] US versus EU anti-terrorist legislation; EU versus US legal privacy regime; European Parliament versus Council and Commission; 'commercial processing' of data versus 'law enforcement processing'; and data protection versus data mining.

In the aftermath of the 11 September 2001, terrorist attacks, the US government adopted legislation requiring airlines flying into US territory to transfer to designated US authorities data relating to passengers and cabin crew and contained in the so-called 'Passenger Name Record'.

The Passenger Name Record is a computerised record of each passenger's travel requirements which contain all information necessary to enable reservations to be processed and controlled by the airlines. PNR datasets may be composed of as many as 60 data fields[6] and can also contain information on individuals who are not travelling by air, such as, the details (e-mail address, telephone number) for contacting a person (e.g. a friend or a family member). PNR data may reveal religious or ethnic information (for example, from the meal preferences of the passenger), affiliation to a particular group, as well as medical data (for example medical assistance required by the passenger, or any disabilities or health problems that are made known to the airline). The purpose for collecting the PNR data is to identify individuals who may pose a threat to the US aviation safety or national security.

Air carriers' failure to forward the required PNR data was punishable with loss of landing rights in the US and the payment of fines. European airline companies, therefore, found themselves between a rock and a hard place because if they gave in to the US authorities' demands, they would violate EU data protection law[7] and if they followed EU law they were liable to US sanctions.

The first PNR agreement negotiated between the EU and the US administration was concluded on 28 May 2004.[8] The agreement was challenged by the European Parliament (EP), which argued that it violated fundamental human rights as protected in the EU, and was annulled in 2006 by the European Court of

---

[4] Andrew Rettman, 'EU Should Create Own Spy Agency, Reding Says' *euobserver* (4 November 2013), <http://euobserver.com/justice/121979> accessed 3 November 2014.

[5] Megan Roos, 'Definition of the Problem: The Impossibility of Compliance with Both European Union and United States Law' (2005) 14 Transnat'l L. & Contemp. Probs. 1137, 1138.

[6] These data fields include: name, address, e-mail, contact telephone numbers, passport information, date of reservation, date of travel, travel itinerary, all forms of payment information, billing address, frequent flyer information, travel agency and travel agent, travel status of passenger (such as confirmations and check-in status), ticketing field information (including ticket number, one-way tickets and Automated Ticket Fare Quote), date of issuance, seat number, seat information, general remarks, no show history, baggage information, go show information, OSI (Other Service-related Information) and SSI/SSR (Special Service Information/Special Service Requests).

[7] Article 25 (1) of the Data Protection Directive prohibits the transfer of personal data to third countries that do not ensure an 'adequate level of protection'.

[8] Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004 L 183/ 83 and corrigendum at OJ 2005 L 255/168. The Council's decision was based on the Commission's adequacy finding. *See* Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection, OJ 2004 L 235/11.

Justice (ECJ)[9] on the rather technical ground that it was adopted on the wrong legal basis. The EU entered subsequently into an Interim Agreement[10] until a new PNR Agreement was signed with the US on 23 July 2007.[11] The negotiations for the latest PNR Agreement began in 2011 and the current EU-US PNR Agreement[12] entered into force in June 2012 and is due to expire in seven years. The EU-US PNR agreements have sparked a heated debate in Europe regarding their compatibility with the fundamental rights to privacy and data protection with the European Parliament and the Article 29 Working Party having repeatedly raised their concerns on the issue.

2. EU-US: Two Different Cultures of Privacy?

2.1 Dignity, Liberty and Other Misconceptions of Privacy

It has been argued in both sides of the Atlantic, that 'the drama that played out between the United States and the European Union over PNR-data transfers is a prominent example of the clash between conflicting philosophies on privacy protection.'[13] An American scholar criticised the 'strict' pro-privacy stance adopted by the EU in the PNR negotiations noting that 'increased information sharing is the best way of preventing terrorism, but information sharing between the public and private sector may be difficult if Americans are focused on the dangers of state surveillance and Europeans are concerned about protecting the dignity of the consumer.'[14]

While such a contention would raise eyebrows in Europe, it reflects a perception that is far from rare in American literature. Legal historian James Whitman, argued in Yale Law Journal in 2003, that 'American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity.'[15] According to Whitman, European privacy law, being based on personal dignity, focuses on the protection of rights such one's image, name, reputation, and informational self-determination.[16] Whitman, therefore, identified the media as the prime enemy of the right to privacy in the European continental conception.[17] By contrast, America, according to the same author, 'is much more oriented toward values of liberty, and especially liberty against the state.'[18] In essence, at the conceptual core of the American right to privacy lies 'the right to freedom from intrusions by the state, especially in one's own home.'[19]

Whitman's argument is based on the historical analysis of the evolution of the right to privacy in Germany and France and suffers from a number of fallacies. First, it fails to acknowledge that Europe or the EU is not only Germany and France. Second, European privacy and data protection law has vertical and horizontal application, in that it applies against the state (as a non-interference protective rule) and against other individuals. To argue, therefore, that Europeans are concerned about protecting 'the dignity of the consumer'

---

[9] Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission (PNR)* [2006] ECR I-4721. For an analysis, *see* Jorrit J Rijpma and Gráinne Gilmore, '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' [2007] 44 Common Market Law Review 1081, 1087.

[10] Council Decision 2006/729/CFSP/JHA of 16 October 2006 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security, OJ L 298/27 of 27 October 2006.

[11] 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 Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L 204/16 of 4 August 2007.

[12] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security (2012 PNR Agreement) (adopted 14 December 2011, entered into force 1 July 2012) OJ L 215/5, 11/08/2012.

[13] Arthur Rizer, 'Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber' (2010) 60 Cath. U. L. Rev. 77, 79. According to Rasmussen, 'The dispute between the United States and European Union over the transfer of PNR data is a *prima facie* conflict of laws dispute.' Richard Rasmussen, 'Is International Travel per Se Suspicion of Terrorism? The Dispute between the United States and European Union over Passenger Name Record Data Transfers' (2009) 26 Wis. Int'l L.J. 551, 588. *See* also Fernando Mendez and Mario Mendez, 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States' (2009) 40 Publius: The Journal of Federalism 617; Allen Shoenberger, 'Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead' (2007) 17 Ind. Int'l & Comp. L. Rev. 375.

[14] Jeffrey Rosen, 'Continental Divide: Americans See Privacy as a Protection of Liberty, Europeans as a Protection of Dignity. Will One Conception Trump the Other—or Are Both Destined to Perish?' [2004] Legal Affairs <http://www.legalaffairs.org/issues/September-October-2004/review_rosen_sepoct04.msp>; Timothy Ravich, 'Is Airline Passenger Profiling Necessary?' (2007) 62 U. Miami L. Rev. 1, 49.

[15] James Q Whitman, 'Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal 1151, 1163.

[16] Ibid 1167.

[17] Ibid 1171.

[18] Ibid 1161.

[19] Ibid 1162.

is, at best, an inaccurate generalisation.[20] Setting aside such misconceptions, a closer examination of the EU and the US privacy regimes reveals that as far as standards of protection are concerned, these are in fact two different cultures of privacy.

2.2 The EU privacy regime

The right to privacy enshrined in Article 8 of the European Convention on Human Rights (ECHR) has been recognised as a general principle of EU law and is now entrenched as a fundamental right in Article 7 of the EU Charter of Fundamental Rights (EUCFR).[21] Furthermore, the EU legal order recognises data protection as a fundamental right in Article 8 EUCFR.[22] Data protection was born out of the concerns raised in different European countries in the 1970s about the establishment of huge data banks and the increasingly centralised processing of personal data.

The EU's data protection legislation is considered the most ambitious, comprehensive and complex regime worldwide.[23] The first data protection legal instrument in the EU, the Data Protection Directive was adopted in 1995. Since then, further legislation was enacted for the protection of privacy in the electronic communications sector (the e-Privacy Directive),[24] the processing of personal data by the EU institutions (Regulation 45/2001/EC),[25] and the retention of telecommunications metadata (the Data Retention Directive), which was (rather surprisingly) presented as a modification of EU data protection legislation.

The Data Protection Directive (Directive 95/46/EC) (the Directive) constitutes the central legislative measure of the EU data protection regime. Its aim is twofold: on the one hand, to protect privacy with respect to the processing of personal data; on the other hand, to ensure the free movement of personal data in the EU. The Directive sets out a number of principles concerning the legitimate processing of personal data, normally referred to as 'data protection' or 'fair information principles'. It is the obligation of the so-called 'controller' to comply with these principles. The Directive provides for increased protection for 'sensitive data' that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning sex or health life.[26] Furthermore, the Data Protection Directive lays down a number of rights of the data subject, which are primarily procedural, such as the right to information,[27] right of access,[28] and right to object to the processing of their data.[29] Compliance of the controllers with the Directive is ensured by independent authorities in the territory of each Member State (the National Data Protection Authorities (NDPAs)). The National Data Protection Authorities are endowed with investigative powers, powers of intervention, and the power to engage in legal proceedings where the national data protection law implementing the Directive has been violated. The Directive also establishes an independent EU Advisory Body on the protection of individuals with regard to the processing of personal data, normally referred to as the 'Article 29 Working Party',[30] which is composed of representatives of NDPAs, the European Data Protection Supervisor, and the Commission. Its main task is providing expert opinions to the Commission on various data protection questions. Even though the Article 29 Working Party has only advisory competences, it has played an important role in promoting data protection issues within the EU, and has produced a significant number of reports, recommendations and opinions on privacy matters.

Since the adoption of the Data Protection Directive, the Court of Justice of the EU (CJEU) has been called upon several times to rule on questions of interpretation and application of this instrument. If we attempt

---

[20] Vagelis Papakonstantinou and Paul de Hert, 'The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic' (2009) 46 Common Market Law Review 885, 898.

[21] Charter of Fundamental Rights of the European Union.

[22] The constitutional legal basis for measures concerning data protection within the EU is Article 16 of the Treaty on the Functioning of the European Union (TFEU). For a discussion on the relationship between the rights to privacy and data protection *see* M Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88.

[23] Lee A Bygrave, *Data Privacy Law: An International Perspective* (1st edn, Oxford University Press 2014) 53.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201/37 of 31.07.2002.

[25] Regulation (EC) 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1 of 12.1.2001.

[26] Article 8 (1).

[27] Article 10.

[28] Article 12.

[29] Article 14.

[30] Article 29.

a general comment on the Court's reading of the Data Protection Directive, this would be that the CJEU, in essence, has interpreted an internal market harmonisation instrument (the Directive) in a manner that fosters the protection of the fundamental rights to privacy and data protection within the Community.[31] This case-law of the Court culminated with its seminal decision in the joined cases, *Digital Rights Ireland and Seitlinger and others*, which invalidated the Data Retention Directive on the basis that the retention of electronic communications metadata violates the rights to privacy and data protection in the EU.[32]

The Data Protection Directive specifically stipulates that it does not apply to processing operations concerning public security, defence, State security, and the activities of the State in areas of criminal law (Article 3(2)). The processing of data in the area of police and judicial cooperation for the purpose of the prevention, investigation, detection or prosecution of criminal offences is currently governed by Framework Decision 2008/977/JHA. Most of the substantive provisions of the Framework Decision seek to mirror the data protection safeguards stipulated in the Data Protection Directive, but they are either fraught with exceptions or their content is significantly watered down in comparison to these of the Data Protection Directive.[33] Moreover, the scope of application of the Framework Decision is substantially limited. First, it applies only to transborder flows of data between the law enforcement authorities of the Member States, and does not cover the collection and processing of personal data at the national level. Second, it does not affect the relevant set of sector-specific data protection regimes found in the acts governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS). Third, the Framework Decision applies "without prejudice to essential national security interests and specific intelligence activities in the field of national security".[34] Fourth, it is also "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 its adoption.[35]

The EU's data protection legislation is currently under revision. This is because the current legal framework is dated and fragmented with different legal instruments applying to different pillars (the Data Protection Directive in the former first pillar and the Framework Decision in the third pillar). Despite the expectations for a new consolidated data protection framework, the Commission put forward, on 25 January 2012, a proposal package including two separate instruments: A Regulation (aimed to replace the Data Protection Directive), and a Directive (aimed to replace the Data Protection Framework Decision). This proposal package lays down rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The proposals, which are currently been negotiated by the EU institutions, contain many innovative provisions (such as a right to be forgotten in the digital environment and a right to data portability) and will even further strengthen the EU's privacy framework.

2.3 The US privacy regime

Describing the US privacy regime, legal scholar Gregory Shaffer noted: 'data privacy regulation in the United States is fragmented, *ad hoc*, and narrowly targeted to cover specific sectors and concerns.'[36] US privacy law can be found in a number of different sources: the US Constitution, the Supreme Court case law, federal legislation, state legislation and the theory of torts.[37] The Constitutional protection of privacy is mainly based on the First Amendment (protection of free speech and freedom of assembly), the Fourth Amendment (protection from unreasonable searches and seizures), and the Fifth Amendment (privilege against self-incrimination).[38] The Fourth Amendment, in particular, aims in the words of the US Supreme Court, 'to protect personal privacy and dignity against unwarranted intrusion by the State.'[39]

---

[31] Maria Tzanou, 'Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence' in Christina Akrivopoulou and Athanasios Psygkas (eds), *Personal data privacy and protection in a surveillance era : technologies and practices* (Information Science Reference 2011) 284.

[32] Joined Cases C293/12 and C594/12 *Digital Rights Ireland and Seitlinger and others*, judgment of 8 April 2014.

[33] Paul De Hert and Vagelis Papakonstantinou, 'The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – A Modest Achievement However Not the Improvement Some Have Hoped for' (2009) 25 Computer Law & Security Report 403, 411; Bygrave (n 23) 71.

[34] Article 1 (4).

[35] Article 26.

[36] Gregory C Shaffer, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' (2000) 25 Yale Journal of International Law 1, 22.

[37] Papakonstantinou and de Hert (n 20) 892.

[38] Susan Brenner, 'Constitutional Rights and New Technologies in the United States' in Ronald Leenes, Bert-Jaap Koops and Paul De Hert (eds), *Constitutional rights and new technologies : a comparative study* (TMC Asser Press; Distributed by Cambridge University Press 2008) 230.

[39] *Schmerber v. California* [1966] 384 U.S 757.

The Fourth Amendment contains two clauses: the first, the substantive clause, protects against certain government activities; the second, the procedural clause, regulates government power through the process of obtaining a warrant.[40] A warrant can be obtained when there is a 'probable cause' for conducting a search or seizure.[41] In *Katz v. United States*,[42] the Supreme Court established that the protection of the Fourth Amendment against government intrusion applies when an individual has a 'reasonable expectation of privacy.'[43] Justice Harlan, in his concurring opinion in *Katz*, articulated the twofold requirement, known as the 'reasonable expectation privacy test',[44] that triggers the application of the Fourth Amendment: 'first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as "reasonable."'[45] This means, according to Justice Harlan, that 'conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.'[46] A similar statement was made by the majority opinion, which held that 'what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'[47] On this basis, the Court has found that US citizens lack a reasonable expectation in anything they say to a friend,[48] their bank records,[49] and their garbage.[50]

In *Smith v. Maryland*,[51] the Court applied this reasoning on phone records. The police, without a warrant, asked the telephone company to install a pen register[52] to record the numbers dialled from the defendant's home.[53] The Court agreed that there was no reasonable expectation of privacy regarding the numbers someone dials on her phone, because '[t]elephone users... typically know that they must convey numerical information to the phone company; that the company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbour any general expectation that the numbers they dial will remain secret.'[54]

Smith v. Maryland established, therefore, a general rule, according to which, 'if information is in the hands of third parties, then an individual can have no reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply.'[55] In the context of the present discussion, the decision is illuminating for the PNR case. Applying the *Smith v. Maryland* reasoning, PNR data cannot be covered by the Fourth Amendment protection since travellers cannot enjoy any reasonable expectation of privacy of data they, themselves, gave to the airline companies in order to effectuate the ticket reservation.

At the federal level, statutes are 'narrowly tailored to specific privacy problems'.[56] The most significant and the only federal omnibus piece of privacy legislation is the Privacy Act of 1974.[57] The Privacy Act embodies fair information principles in a statutory framework governing the means by which federal agencies collect, maintain, use, and disseminate personally identifiable information. The Privacy Act applies to information that is maintained in a 'system of records.' A system of records is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. While the Privacy Act applies to govern-

---

[40] Daniel J Solove, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (2002) 75 Southern California Law Review 1083, 1118.

[41] Daniel Solove and Paul Schwartz, *Information Privacy Law* (3rd ed, Wolters Kluwer Law & Business; Aspen Publishers 2009) 237.

[42] The decision has been characterized as 'the most important judicial decision on the scope of the Fourth Amendment.' *See* Christopher Slobogin, *Privacy at Risk : The New Government Surveillance and the Fourth Amendment* (University of Chicago Press 2007) 13.

[43] *Katz v. United States* [1967] 389 U.S 347.

[44] Christopher Slobogin and Joseph E Schumacher, 'Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society' (1993) 42 Duke L.J. 727, 731.

[45] *Katz v. United States* (n 43).

[46] Ibid.

[47] Ibid.

[48] *United States v. White* [1971] 401 U.S. 745.

[49] *United States v. Miller* [1976] 425 U.S. 435, 437.

[50] *California v. Greenwood* [1988] 486 U.S. 3.

[51] *Smith v. Maryland* [1979] U.S 735.

[52] A pen register is a device that records outgoing telephone calls.

[53] Solove, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (n 40) 1134.

[54] *Smith v. Maryland* (n 51).

[55] Also known as third party doctrine. *See* Solove, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (n 40) 1135.

[56] Daniel Solove, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stan. L. Rev. 1393, 1440.

[57] Pub. L. No. 93-579, 88 Stat. 1896 (2000) (codified at 5 U.S.C. § 552a).

ment records it is ambiguous as to whether it applies to 'commercial data brokers who supply information to the government'.[58] Furthermore, the Privacy Act applies to US citizens and lawful permanent residents. The Privacy PNR Act safeguards were extended administratively by the EU-US PNR agreements to EU citizens concerning their PNR data. However, the Privacy Act is significantly limited by the so-called 'routine use' exception, according to which information may be disclosed for any 'routine use' if disclosure is 'compatible' with the purpose for which the agency collected the information.[59] PNR data is disclosed by the DHS for 'routine use'.

Finally, another important piece of federal legislation is the Freedom of Information Act (FOIA) adopted in 1966.[60] FOIA permits any person (regardless of nationality or country of residence) access to a US federal agency's records, except to the extent such records (or a portion thereof) are protected from disclosure by an applicable exemption under the FOIA. In the 2007 PNR Agreement, FOIA was also extended to apply to individuals travelling with European airlines. According to DHS, PNR data is not disclosed to the public, but to the data subjects or their agents in accordance with US law.

2.4 The need for a comprehensive framework?

The seriously limited US privacy regime discussed above, creates problems to unimpeded transatlantic data flows. As the PNR experience proved, negotiations were difficult, with data protection differences being at the heart of the conflict.[61] A solution would, therefore, be an international agreement setting down certain data protection guarantees that would govern data exchanges between the two parties in order to raise restrictions on data flows.

On 6 November 2006, the EU-US Justice and Home Affairs Ministerial Troika decided to establish an informal high level advisory group[62] to start discussions on privacy and personal data protection in the context of the exchange of information for law enforcement purposes. On 28 May 2008, the Presidency of the Council of the European Union announced to the Permanent Representatives Committee (COREPER), that the EU-US High Level Contact Group (hereafter HLCG) on information sharing and privacy and personal data protection had finalised its report.

The report, which was made public on 26 June 2008,[63] aimed to identify a set of core principles on privacy and personal data protection, acceptable as 'minimum standards' when processing personal data for law enforcement purposes.[64] These should be included preferably in an international agreement binding both the EU and the US,[65] instead of non-binding instruments or political declarations.[66] Both sides recognised that a binding instrument would provide the greatest level of legal security and certainty, and 'the advantage of establishing the fundamentals of effective privacy and personal data protection for use in any future agreements relating to the exchange of specific law enforcement information that might arise between the EU and the US.'[67]

The HLCG, indeed, agreed on a number of principles. These are: 1) purpose specification and purpose limitation; 2) integrity/data quality; 3) necessity and proportionality; 4) information security; 5) sensitive data; 6) accountability; 7) independent and effective oversight; 8) individual access and rectification; 9) transparency and notice; 10) redress; 11) automated individual decisions; and 12) restrictions on onward transfers to third countries.[68]

---

[58] Chris Hoofnagle, 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement' (2004) 29 N.C.J. Int'l L. & Com. Reg. 595, 622.

[59] Daniel Solove, 'A Brief History of Information Privacy Law' [2006] PROSKAUER ON PRIVACY, GWU Law School Public Law Research Paper No. 215 1, 26; Paul Schwartz, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 Iowa L. Rev. 553, 585; Daniel Solove, 'The Origins and Growth of Information Privacy Law' (2003) 748 PLI/PAT 29.

[60] 5 U.S.C. § 552(a)(3)(A).

[61] Besides PNR, a number of other EU-US Agreements refer to the exchange of personal data. For instance, the Extradition and Mutual Legal Assistance Agreement (2003); the Agreements governing personal data exchange between the United States and Europol (2002) and Eurojust (2006); and the SWIFT Agreement.

[62] The group was composed of senior officials from the Commission, the Council Presidency (supported by the Council Secretariat) and the U.S. Departments of Justice, Homeland Security and State.

[63] Council of the European Union, Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection, 9831/08 JAI 275 DATAPROTECT 31 USA 26.

[64] Ibid at 3.

[65] Ibid at 8.

[66] Ibid at 9.

[67] Ibid at 8.

[68] Ibid at 4.

The main problem was that the two sides seemed to understand differently 'law enforcement purposes',[69] which is central for the agreement. For the EU 'law enforcement purposes' meant use of the personal data 'for the prevention, detection, investigation or prosecution of any criminal offense'. For the US, 'law enforcement purposes' was a somewhat broader notion that comprised 'the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offences or violations.'[70] Nevertheless, the HLCG did not seem to find these differences important. For the HLCG, these two different ways of describing 'law enforcement purposes' 'reflect respective domestic legislation and history but may in practice coincide to a large extent.'[71]

In May 2010, the European Commission, taking up the work done by the HLCG, asked the Council to authorise the opening of negotiations with the United States for an agreement, based on Article 16 TFEU, when personal data is transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters.[72] The Commission noted that the aims of the future EU-US agreement should be fourfold. First, the agreement should ensure a high level of protection of the fundamental rights and freedoms of individuals, in particular, the right to protection of personal data, in line with the requirements of the EUCFR.[73] Second, it should provide a clear and coherent legally binding framework of personal data protection standards. Such a framework should remove the uncertainties and bridge the gaps in protection created in the past because of significant differences between EU and US data protection laws and practices. The agreement itself should therefore, according to the Commission, provide enforceable data protection standards and establish mechanisms for implementing them effectively.[74] Third, the agreement should provide a high level of protection for personal data transferred to and subsequently processed in the US for law enforcement purposes.[75] Finally, the agreement would not do away with the requirement for a specific legal basis for transfers of personal data between the EU and the US, with specific data protection provisions tailored to the particular category of personal data in question.[76] On 29 March 2011, it was announced that the EU and the US opened negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism.[77]

2.5 'Spillovers of privacy' or 'spillovers of security'?

The European privacy model has influenced privacy regulations worldwide.[78] As Professor Graham Greenleaf has aptly noted, 'something reasonably described as "European standard" data privacy laws are becoming the norm in most parts of the world.'[79] In an article in 2000, legal scholar Gregory Shaffer argued that US privacy standards were 'ratcheting up to the level of European data protection standards'.[80] Shaffer explained that this was due to cross-border economic exchange that can help 'leverage standards upward, even in a powerful state such as the United States.'[81] In fact, Shaffer was referring to the US-EU Safe Harbour programme, under which US-based companies may avoid EU data protection restrictions on data transfers if they self-

[69] Ibid at 3.
[70] Ibid at 4.
[71] Ibid.
[72] EUROPEAN COMMISSION, PROPOSITION DE RECOMMANDATION DU CONSEIL AUTORISANT L'OUVERTURE DE NEGOCIATIONS EN VUE D'UN ACCORD ENTRE L'UNION EUROPEENNE ET LES ETATS- UNIS D'AMERIQUE SUR LA PROTECTION DES DONNEES PERSONNELLES LORS DE LEUR TRANSFERT ET DE LEUR TRAITEMENT A DES FINS DE PREVENTION, D'INVESTIGATION, DE DETECTION OU DE POURSUITE D'ACTES CRIMINELS Y COMPRIS LE TERRORISME, DANS LE CADRE DE LA COOPERATION POLICIAIRE ET JUDICIAIRE EN MATIERE PENALE COM (2010) 252/2.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Press Release, 'EU-US Negotiations on an agreement to protect personal information exchanged in the context of fighting crime and terrorism', *European Commission* (29 March 2011) <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/203>.
[78] Maria Tzanou, 'The EU Data Protection Directive as a Model for Global Regimes', in Cassese et al. (eds.) *Global Administrative Law: The Casebook* (3rd Edn, IRPA and IILJ 2012). An author has gone as far as calling this 'the Brussels effect'. *See* Anu Bradford, 'The Brussels effect' (2012) 107 Nw. U. L. Rev. 1.
[79] Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' (2012) 2 International Data Privacy Law 68, 77.
[80] Shaffer (n 36) 1. *See* also Chuan Sun, 'The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2 Nw. J. Tech. & Intell. Prop. 99.
[81] Shaffer (n 36) 5.

certify that they abide with certain data protection principles.[82] Shaffer contended that in this way, Europe's regulatory approach may have 'spillover effects within the United States, leading to some convergence in data privacy practices, despite differing US and EC regulatory systems.'[83]

It seems, however, that the privacy regulatory convergence suggested by Shaffer finds its limits when interests such as policing and national defence come into play.[84] A close look to the on-going negotiations between the EU and the US on the conclusion of a binding international agreement on data protection principles in the field of law enforcement shows that even if such an agreement is concluded sometime in the future it is highly unlikely that it will have spillovers in the US privacy regime and result in a levelling up of its privacy standards in the area. There are several points that support this. In its report on the negotiations with the US in 2011, the Commission noted, first, that regarding the purpose of the agreement the US has a mandate for no more than an 'Executive agreement' that does not change existing US law, nor create any new rights.[85] On the material scope of the agreement, the US has rejected the idea to also apply the agreement to data transferred from private parties in the EU to private parties in the US and subsequently processed for law enforcement purposes by US competent authorities. The fear of potential European privacy spillovers in the other side of the Atlantic is also evident when it comes to the data subjects' rights in the negotiated agreement. Their content is clearly watered down in comparison to EU standards. Regarding the right to information and the right to access of the data subjects, the US side has defended its existing system and opposed the idea of changing its legislation in order to provide for such rights in the law enforcement context. The same goes regarding the right to redress, for which the US has argued that it is adequately safeguarded in its current legislation and in any case the creation of any individual rights will not be accepted.[86]

While any spillovers of privacy seem very unlikely even if the agreement is concluded in the future, the other side of the coin is that in its counter-terrorism fight the EU is looking more towards the US than the other way round. As an American author predicted already in 2002 'since EU and US political interests are largely aligned [...] against terrorism, it is possible that the European Union will move closer to the United States as a result of the [September 11] attacks, rather than the United States moving away from the European Union. To the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programmes.'[87]

PNR is a prominent example of this. Despite the apparent clash, the EU is already moving towards the establishment of its own PNR system. While potential 'spillovers of privacy' are not visible yet, 'spillovers of security,' looking in the opposite direction, are certainly here.

3. Outside Bad, Inside Good: The EU PNR Arrangement

3.1 The Proposal for an EU PNR Framework Decision

The European Council in the Stockholm Programme invited the Commission to present a proposal on the establishment of an EU PNR system.[88] Following this, on 6 November 2007, the Commission introduced its proposal for a Council Framework decision on the use of PNR for law enforcement purposes under the then third pillar.[89] The draft Framework decision had as its purpose 'the making available by air carriers of PNR data of passengers of international flights to the competent authorities of the Member States, for the purpose of preventing and combating terrorist offences and organised crime.'[90] For this reason, the Framework decision required each Member State to designate a competent authority ('Passenger Information Unit' ('PIU')), which would be responsible for collecting the PNR data of international flights arriving or depart-

[82] For an overview of the EU-US Safe Harbor Agreement *see* Export.gov <http://export.gov/safeharbor/eu/eg_main_018365.asp>.

[83] Gregory C Shaffer, 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements' (2002) 9 Colum. J. Eur. L. 29, 57.

[84] Francesca Bignami, 'European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' (2007) 48 Boston College Law Review 609, 676.

[85] COUNCIL OF THE EUROPEAN UNION 5999/12 LIMITE JAI 53 USA 2 DATAPROTECT 13 RELEX 76, Brussels, 3 February 2012.

[86] Professor Paul Schwartz is categorical on this issue: '[T]he United States never enacted EU-style privacy legislation nor created EU-style institutions.' *See* Paul M. Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harvard Law Review 1966, 1985.

[87] Steven Salbu, 'The European Union Data Privacy Directive and International Relations' (2002) 35 Vand. J. Transnat'l L. 655, 694. For a more recent account s*ee* Joel Reidenberg, 'The Data Surveillance State in the United States and Europe' (2014) 49 Wake Forest L. Rev. 583.

[88] European Council, The Stockholm Programme- An Open and Secure Europe Serving and Protecting Citizens, OJ C115/1 of 4.5.2010, at 19.

[89] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes COM(2007) 654 final.

[90] Article 1.

ing from its territory.[91] The PIU would further be responsible for analysing the PNR data and for carrying out a risk assessment of the passengers, in order to: identify persons, and their associates, who are or may be involved in a terrorist or organised crime offence; create and update risk indicators for the assessment of such persons; provide intelligence on travel patterns and other trends relating to terrorist offences and organised crime; use the risk assessment in criminal investigations and prosecutions of terrorist offences and organised crime.[92]

The PNR data to be transmitted according to the draft Framework decision were almost identical to the categories listed in the then EU-US PNR Agreement.[93] The draft Framework decision required nineteen data fields exactly as the 2007 PNR Agreement, which appeared to be its model legislation. Air carriers would be required to make available the data to the relevant PIU twice—24 hours before the scheduled flight departure, and immediately after flight closure.[94] The PNR data would be retained for a period of thirteen years in total: for five years in a PIU database and subsequently for another eight years, during which access would be limited to exceptional circumstances.[95] Concerning the data protection principles applicable to the EU PNR system, the draft Framework decision could not be briefer. Two articles referred to data protection, one of which one was dedicated to data security.[96] The other prohibited any enforcement action to be taken by the PIUs or the Member States based only on the the automated processing of PNR data or by reason of a person's race or ethnic origin, religious or philosophical belief, political opinion or sexual orientation.[97]

3.2 Behind the proposal: Why an EU PNR system?

It is, at the very least, puzzling that the EU is envisaging establishing its own PNR scheme.[98] This is all the more if one recalls the EU objections to the relevant US initiatives and the controversies that surrounded the EU-US PNR negotiations. Furthermore, when the proposal for an EU PNR was tabled, the EU already had a system in place for collecting the so-called API data.[99] In particular, Directive 2004/82/EC requires air carriers to transmit the information included in the machine-readable part of a passport (API data), in order to combat illegal immigration and improve border control.[100] The use of API data for law enforcement purposes is also permitted by the Directive under certain conditions.[101] Personal data, therefore, such as name, gender, data of birth, nationality, type of travel document, departure and arrival time of transportation, the border crossing point of entry into the territory of the EU Member States, and the initial point of embarkation of passengers entering the EU were already available through the API system.

It is not only the EU PNR system proposal that surprises; it is also that this is in many areas almost 'the exact mirror of the transatlantic PNR system.'[102] The data categories to be retained, the retention arrangements that recall the US 'active' and 'dormant' database distinction, the periods of the retention,[103] and the purposes of the PNR collection uncannily remind one of the EU-US PNR Agreement.[104] The question is therefore: why is an EU PNR system which all the more looks like a replica of the US Agreement so vigorously opposed?

---

[91] Article 3.

[92] Article 3 (5).

[93] House of Lords European Union Committee, 'The Passenger Name Record (PNR) Framework Decision' 15th Report of Session 2007-08, para 22.

[94] Article 5.

[95] Article 9.

[96] Article 11 (Protection of personal data) and Article 12 (Data security).

[97] Article 11 (3).

[98] Patryk Pawlak, 'Made in the USA ? The Influence of the US on the EU 's Data Protection Regime' (2009) CEPS 5.

[99] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261/24 of 6.8.2004.

[100] Article 1.

[101] Article 6 (1).

[102] Javier 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, 130.

[103] Concerning the data retention period the EDPS noted in his Opinion on the Framework decision: 'the period of 13 years is comparable to the retention period of 15 years in the most recent agreement with the United States. The EDPS has always understood that this long retention period was only agreed upon because of strong pressure by the US Government to have a much longer period than 3.5 years, not because it was in any stage defended by the Council or the Commission. There is no reason to transpose such a compromise —that only has been justified as a necessary result of negotiations — to a legal instrument within the EU itself.' *See* Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes OJ C 110/1 of 1 May 2008, para 103.

[104] As Article 29 Working Party elegantly put it 'The proposal is closely modelled on the EU-US PNR agreement signed in July 2007 and many features of the present draft are similar to that agreement.' *See* Article 29 Working Party, Working Party on Police and Justice, 'Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Presented by the Commission on 6 November 2007'.

The reasons that the Commission gave in its Explanatory Memorandum seem 'a little ambiguous'.[105] It started by explaining that only a limited number of Member States had adopted a PNR system, and thus 'the potential benefits of an EU wide scheme in preventing terrorism and organised crime [were] not fully realised.'[106] At the time of the proposal, the UK was the only country in the EU collecting PNR data.[107] According to the Commission's Explanatory Memorandum, 'the UK was able to report numerous arrests, identification of human trafficking networks and gaining of valuable intelligence in relation to terrorism in the two years of the operation of its pilot [PNR] project.'[108] A more specific account of these alleged successes of PNR in the UK was, however, missing in the Explanatory Memorandum. Denmark and France had also laid down relevant legislation, but they were not collecting any data yet. Surprisingly enough, the Commission spoke then of the need for a harmonised approach concerning PNR: 'Action by the EU will better achieve the objectives of the proposal because a harmonised approach makes it possible to ensure EU wide exchange of the relevant information.'[109]

Furthermore, the Commission appeared convinced of the necessity of a PNR system as a counter-terrorism tool because of its 'worldwide acceptance': the use of PNR data is 'increasingly seen as a mainstream and necessary aspect of law enforcement work.'[110] This trend is, according to the Commission, the result of three parameters. First, international terrorism and crime are serious threats to society that should be dealt with. Second, recent technological developments have rendered access and analysis of travel data possible, and lastly, with the rapid increase of international travel and the volume of passengers, electronic data processing in advance of passengers' arrivals 'largely facilitates and expedites security and border control checks since the risk assessment process is done before arrival'. According to the Commission, the analysis of PNR data provides the opportunity to law enforcement to focus only 'on those passengers for whom they have a fact-based reason to believe that they might pose an actual risk to security, rather than making assessments based on instinct, pre-conceived stereotypes or profiles.'[111]

These justifications are not very convincing as empirical evidence on PNR system effectiveness is lacking and, in any case, the need for a harmonised approach regarding the collection of PNR data in the EU is far from proven. So, what are the true reasons behind the development of an EU PNR system?

First of all, one should not underestimate the EU's quest for reciprocity. All the three EU-US PNR Agreements concluded by the time of the Commission's PNR proposals contained a reciprocity clause, according to which the EU might develop its own PNR system in the future.[112] The wording was almost identical: 'In the event that a PNR system is implemented in the European Union ... [the] DHS shall, strictly on the basis of reciprocity, actively promote the cooperation of the airlines within its jurisdiction.'[113]

Since 2003, the Commission aspired to develop an EU PNR scheme.[114] The rationale was that such a system would form the basis for the establishment of an information policy for law enforcement authorities, which would become the backbone for a prevention policy in the field of organised crime and terrorism.[115]

Moreover, one cannot disregard the fact that all the EU-US PNR Agreements display an asymmetry of power[116] or some form of 'unilateralism'. In practice, the agreements are not about the *exchange* of PNR data, but only the '*one-way* access of US government agencies to European data.'[117] The quest for reciprocity seems, therefore, justifiable for the EU. As eloquently put by one Commission official 'it would have been difficult to explain to European passengers that US authorities would receive more information than

[105] Evelien Brouwer, 'The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?' (2009) CEPS Working Document No 320 25.

[106] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, at 2.

[107] House of Lords European Union Committee, 'The Passenger Name Record (PNR) Framework Decision' (n 93), 5.

[108] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 2.

[109] Ibid at 7.

[110] Commission Communication On the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, 3.

[111] Ibid at 5.

[112] Undertaking 45 and Article 6 of the 2004 PNR Agreement; Article 5 of the 2006 (Interim) PNR Agreement; and, Article 5 of the 2007 PNR Agreement.

[113] Article 5 of the 2007 PNR Agreement. The wording differs only slightly in the 2004 Agreement.

[114] On 9 October 2003 an experts' meeting was organised by the Commission, with the participation of law enforcement and data protection authorities of the Member States, in order to discuss the establishment of an EU PNR system.

[115] Communication from the Commission to the Council and the Parliament, Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach, Brussels, 16 December 2003 COM(2003) 826 final.

[116] Argomaniz, (n 102), at 126–127.

[117] Bert-Jaap Koops, 'Law, Technology, and Shifting Power Relations' (2010) 25 Berkeley Tech. L.J. 973, 987.

their own national services.'[118] In his Oral Evidence to the House of Lords Jonathan Faull, the then Director-General for Justice, Freedom and Security, stated: 'The Commission›s view is that it would make sense to have a PNR system for ourselves in the European Union on the basis of which we would then have very good grounds for saying to our American partners, "This must be completely reciprocal. We have our PNR system, you have yours".'[119]

Some political scientists[120] have argued that the negotiation processes with the US authorities had an impact on the EU institutions, such as the Commission, taking part in them. This might also be the case. As the Commission admitted in the Explanatory Memorandum, on the basis of an exchange of information with the US, 'the EU has been able to assess the value of PNR data and to realise its potential for law enforcement purposes.'[121] This could be further illustrated by the fact that an EU PNR system was supported by the EU negotiating agents (i.e. the Commission and the Presidency), but not by other EU actors, such as the EP or the Article 29 Working Party and the European Data Protection Supervisor (EDPS), who had been kept almost excluded from the negotiations with the US.[122]

3.3 The reaction of the outsiders

The proposal of a Framework decision establishing an EU PNR regime was received with fierce criticisms by the Article 29 Working Party, the EDPS, the Fundamental Rights Agency (FRA), and the European Parliament. In particular, the Article 29 Working Party in its joint opinion with the Working Party on Police and Justice characterised the proposal as 'a further milestone towards a European surveillance society in the name of fighting terrorism and organised crime.'[123]

In fact, the reaction of the above institutions and bodies was even more severe than the criticisms they voiced for the EU-US PNR Agreements. Both the Working Party and the EDPS demanded that an EU PNR system must be 'demonstrably necessary.'[124] The necessity of the EU-US PNR Agreements was also questioned, but given the position of the European airlines and the pressure exercised by the US authorities for the prompt conclusion of an agreement, the Working Party, the EDPS, and the Parliament were focusing more on the substantial assessment of the relevant provisions interfering with the right to data protection. Having to deal with an EU measure this time, their position became clearly stricter: the Commission had to prove beyond doubt the added value of an EU PNR system.[125]

Another criticism raised against the proposal by all four institutions concerned the profiling aspirations of the EU PNR regime. As the EDPS noted eloquently, contrary to the API data that are supposed to help identify individuals, PNR data 'would contribute to carrying out risk assessments of persons, obtaining intelligence and making associations between known and unknown people.'[126] The purpose of a PNR system does not only cover the catching of *known* persons but also the locating of persons that may be of interest for law enforcement reasons.[127] A substantial part of FRA's Opinion concerning the draft PNR Framework decision is dedicated to a human rights assessment of the 'profiling purposes' of the proposal, mainly on the basis of the prohibition of discrimination found in Article 21 EUCFR.[128] The European Parliament also raised similar concerns in its Resolution.[129]

---

[118] *See* Argomaniz, (n 102), at 130.

[119] House of Lords European Union Committee, 'The Passenger Name Record (PNR) Framework Decision' (n 93), para 150.

[120] *See* for instance Argomaniz, (n 102), at 130.

[121] Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, at 2.

[122] Argomaniz, (n 102), at 132.

[123] Article 29 Working Party, Working Party on Police and Justice, Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement purposes, presented by the Commission on 6 November 2007.

[124] Ibid at 5.

[125] Ibid at 6.

[126] Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes OJ C 110/1 of 1 May 2008, para 6.

[127] Ibid para 15.

[128] Fundamental Rights Agency, 'Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes' (2008) 7 <http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf> accessed 15 October 2011.

[129] European Parliament resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name Record (PNR) for law enforcement purposes P6_TA(2008)0561.

Finally, there were numerous problems identified in the proposal: the excessive categories of data to be retained,[130] the disproportionate retention periods,[131] the uncertainty on the individuals' rights,[132] the questions on the applicable legal framework,[133] and the role of PIUs and intermediaries.[134]

3.4 The proposal for an EU PNR Directive: A step forward?

Upon the Lisbon Treaty's entry into force on 1 December 2009, the Commission's proposal of 6 November 2007 for a Framework decision on PNR, which had not been adopted by the Council by that date, became obsolete. On 2 February 2011, the Commission introduced a new proposal on the establishment of an EU PNR system – this time for a Directive.[135] The proposal was based once again on the need for harmonisation of the Member States relevant provisions. This time, however, the Commission seemed slightly more convincing. According to the Explanatory Memorandum, the UK already had its PNR system, while France, Denmark, Belgium, Sweden and the Netherlands had either enacted relevant legislation or were testing using PNR data. The Commission explained that it carried out an impact assessment for the development of an EU PNR system which concluded that a legislative proposal with decentralised PNR data collection for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and other serious crime was the best policy option.[136]

Under the proposed Directive, Member States are, once again, required to establish a single designated unit (PIU) responsible for handling and protecting the data.[137] The categories of PNR data to be transmitted are the same 19 elements found in the draft Framework decision. Air carriers are obliged to transmit the PNR data 24 to 48 hours before the scheduled time for flight departure, and immediately after flight closure.[138] The data is to be retained for a period of five years: initially for 30 days after their transfer to the relevant PIU, and subsequently, after being masked out and made anonymous they will be held for another five years.[139] The draft Directive prohibits the collection and use of sensitive data, such as data revealing racial or ethnic origin, political and religious beliefs, health and sexual life.[140] It obliges carriers to transmit PNR data exclusively by the "push" method, meaning that the Member States will not have direct access to the carriers' IT systems.[141] The result of the processing of PNR data by a PIU should be exchanged, where necessary, with the PIUs of other Member States.[142] The national data protection authorities will be responsible for advising and monitoring how PNR data is processed.[143]

Concerning the data protection safeguards, the draft Directive is even more economical than the draft Framework decision: it merely states that every passenger would have the same right to access, rectification, erasure and blocking, compensation and judicial redress as those adopted under national law in implementation of Articles 17, 18, 19 and 20 of the Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters.[144] Member States are further required to ensure that passengers are clearly and precisely informed about the collection of PNR data and their rights.[145] Finally, the draft Directive prohibits the transfer of PNR data by PIUs and competent authorities to private parties in Member States or in third countries.[146] It must be acknowledged that the Commission has been very careful concerning the drafting of the Directive on PNR in an attempt to address the severe criticisms raised against the draft Framework decision. In this respect, it has taken great pains to prove that a PNR system at the EU level has indeed an added value. However, its analysis on the necessity

130 Article 29 Working Party, Working Party on Police and Justice, Joint Opinion on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement purposes (n 123).
131 Ibid.
132 Ibid.
133 Opinion of the European Data Protection Supervisor on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (n 126), para 39.
134 Ibid. at para 68.
135 Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime COM(2011) 32 final.
136 Ibid.
137 Ibid. Article 3.
138 Ibid. Article 6.
139 Ibid. Article 9.
140 Ibid. Article 11 (3).
141 Ibid. Article 6 (1).
142 Ibid. Article 7.
143 Ibid. Article 12.
144 Ibid. Article 11 (1).
145 Ibid. Article 11 (5).
146 Ibid. Article 11 (6).

of an EU PNR system, despite being clearly more elaborate than the one provided in the draft Framework decision, fails, once again, to convince.[147]

Regarding the substance, despite some visible improvements compared to the draft Framework decision, such as, for instance, the reduced retention period, the implementation of a 'push' system, and the exclusion of any collection and processing of sensitive data, the draft Directive does not add much. In particular, it is lamentable that the data protection legal framework applicable to the PNR Directive is the Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters, even in the post-Lisbon context.

The proposal is currently being debated by the Council and the EP. The Council has introduced two further restrictive amendments. First, the collection of PNR data should not be limited to flights from and to third countries, but should also cover flights operating within the EU. Such possibility should be given to the Member States that would require these data as well. Second, the Council considers that an initial retention period of 30 days, as provided in the Commission's proposal, is 'too short from an operational point of view' and this should be prolonged to two years.

The debate of the draft Directive on an EU PNR system has not been concluded in the Parliament yet, but the LIBE Committee voted on 29 April 2013 against the proposal and called the European Parliament to reject it and the Commission to withdraw it. In particular, the LIBE Committee voiced its concerns regarding the compatibility of an EU PNR scheme with the fundamental right to data protection enshrined in Article 8 EUCFR and the principle of proportionality. Also, the Committee was not convinced of the effectiveness of the PNR data in order to fight terrorism.[148] The EP has not voted on the proposed PNR Directive yet and it seems that the issue has stalled at least temporarily.

However, it seems that the political institutions of the EU have not forgotten it. In its Special Meeting of 30 August 2014, the European Council called the Council and the EP to finalise work on the EU PNR proposal before the end of 2014.[149] The European Council deemed that this was necessary in the context of the action that needs to be taken in order to detect and disrupt suspicious travel and investigate and prosecute foreign fighters.

3.5 The paradox of the EU's approach to fighting terrorism

The EU's proposals to create a Passenger Name Record system shows a fundamental paradox emerging in the EU's fight against terrorism. The EU itself maintains that it is an entity based on the rule of law that respects human rights.[150] As some commentators have observed, the EU has successfully constructed the image of itself as a 'moral leader of good'[151] in the fight against terrorism due to its alleged higher respect to human rights standards compared to the US. Taking this into account as well as the severe criticisms that have been raised against the EU-US PNR system, one would expect increased constitutional and human rights safeguards to be adopted by the EU as a response to the US' struggle against terrorism in order to counteract the constitutional challenges posed by the international counterterrorism pressures. Instead, it seems that the contrary is taking place, in that external security measures are followed by proposals for the internalisation of the same or similar internal security measures that erode further the EU's constitutional framework. Moreover, the PNR proposal does not contain strict human rights mechanisms but rather appears to be a poor copy of the much-criticised international agreement. This paradox illuminates the new dynamics that arise in the EU's fight against terrorism. Privacy and data protection as well as human rights in general are now taking a back seat to the new security initiatives that normally go hand in hand with security spillovers. In this respect, the EU seems to be following 'an eye for an eye' approach in its fight against terrorism. If European PNR data is transferred to the US or other countries, the EU should request the same data from these countries as well. A race to the bottom concerning the right to privacy

---

147 Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Brussels, 25 May 2011 at para 10; Article 29 Working Party, 'Opinion 10/2011 on the Proposal for a Directive of the European Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime'.

148 Marine Marx, 'The EP Committee Rejects the Proposal for an European Passenger Name Record System (PNR)' (*European Area of Freedom Security & Justice,* 1 May 2013) <http://free-group.eu/2013/05/01/the-ep-committee-rejects-the-proposal-for-an-european-passanger-name-record-system-pnr/#_ftn5> accessed 4 November 2014.

149 Conclusions of the Special Meeting of the European Council of 30 August 2014, EUCO 163/14 CO EUR 11 CONCL 4, para 18.

150 *See* Consolidated version of the Treaty on European Union [2012] OJ C326/01, Article 2.

151 Natalia Chaban, Ole Elgstrom and Martin Holland, 'The European Union as Others See It' (2006) 11 European Foreign Affairs Review 245, 259.

appears, therefore, to be taking place in the name of the fight against terrorism, with the US leading and the EU following suit.

Conclusion

The transatlantic war against terror has demonstrated a growing divide between the EU and the US in the field of privacy and the fight against international terrorism. Measures, such as the transfer of PNR data, have been fiercely resisted in the EU because they seriously interfere with European privacy standards. This divide has been attributed by many to the idea that the EU and the US have two different cultures of privacy. The present contribution has argued that this is true to the extent that the EU privacy framework, despite its shortcomings, is clearly more protective than the US privacy regime.

The adoption of a transatlantic privacy agreement governing the exchange of personal data for law enforcement purposes could be a solution to the transatlantic privacy divide. Such an agreement could even raise hopes regarding the levelling up of privacy standards in the US. However, the reality seems to be different. The US is not willing to accept the creation of any new individual privacy rights and the agreement itself is far from being adopted yet.

While spillovers of privacy are nowhere to be seen, spillovers of security are certainly here. The EU PNR proposal is an eminent example of the paradox emerging in the EU's fight against terrorism. Despite having severely criticised the collection of PNR data by the US, the EU has followed suit by proposing to internally adopt a very similar security measure. In this respect, the European Parliament is the only institution that can put a halt to this race to the bottom regarding the right to privacy in the fight against terrorism.

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

Bignami F, 'European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' (2007) 48 Boston College Law Review 609

Brenner S, 'Constitutional Rights and New Technologies in the United States' in Ronald Leenes, Bert-Jaap Koops and Paul De Hert (eds), Constitutional rights and new technologies : a comparative study (TMC Asser Press; Distributed by Cambridge University Press 2008)

Brouwer E, 'The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?' (2009) CEPS Working Document No 320

Bygrave LA, Data Privacy Law: An International Perspective (First edition, Oxford University Press 2014) DOI: http://dx.doi.org/10.1093/acprof:oso/9780199675555.001.0001

Chaban N, Elgstrom O and Holland M, 'The European Union as Others See It' (2006) 11 European Foreign Affairs Review 245

Hoofnagle C, 'Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement' (2004) 29 N.C.J. Int'l L. & Com. Reg. 595

Koops B-J, 'Law, Technology, and Shifting Power Relations' (2010) 25 Berkeley Tech. L.J. 973

Marx M, 'The EP Committee Rejects the Proposal for an European Passenger Name Record System (PNR)' <http://free-group.eu/2013/05/01/the-ep-committee-rejects-the-proposal-for-an-european-passanger-name-record-system-pnr/#_ftn5> accessed 4 November 2014

Mendez F and Mendez M, 'Comparing Privacy Regimes: Federal Theory and the Politics of Privacy Regulation in the European Union and the United States' (2009) 40 Publius: The Journal of Federalism 617

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

Pawlak P, 'Made in the USA ? The Influence of the US on the EU 's Data Protection Regime' (2009) CEPS

Rasmussen R, 'Is International Travel per Se Suspicion of Terrorism? The Dispute between the United States and European Union over Passenger Name Record Data Transfers' (2009) 26 Wis. Int'l L.J. 551

Ravich T, 'Is Airline Passenger Profiling Necessary?' (2007) 62 U. Miami L. Rev. 1

Rettman A, 'EU Should Create Own Spy Agency, Reding Says' <http://euobserver.com/justice/121979> accessed 3 November 2014

Rijpma JJ and Gilmore G, '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' (2007) 44 Common Market Law Review 1081

Rizer A, 'Dog Fight: Did the International Battle over Airline Passenger Name Records Enable the Christmas-Day Bomber' (2010) 60 Cath. U. L. Rev. 77

Roos M, 'Definition of the Problem: The Impossibility of Compliance with Both European Union and United States Law' (2005) 14 Transnat'l L. & Contemp. Probs. 1137

Rosen J, The Unwanted Gaze : The Destruction of Privacy in America (1st Vintage Books ed, Vintage Books 2001)

——, 'Continental Divide: Americans See Privacy as a Protection of Liberty, Europeans as a Protection of Dignity. Will One Conception Trump the Other—or Are Both Destined to Perish?' [2004] Legal Affairs

Salbu S, 'The European Union Data Privacy Directive and International Relations' (2002) 35 Vand. J. Transnat'l L. 655

Schwartz P, 'Privacy and Participation: Personal Information and Public Sector Regulation in the United States' (1995) 80 Iowa L. Rev. 553

Shaffer GC, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards' (2000) 25 Yale Journal of International Law 1

——, 'Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements' (2002) 9 Colum. J. Eur. L. 29

Shoenberger A, 'Privacy Wars: EU Versus US: Scattered Skirmishes, Storm Clouds Ahead' (2007) 17 Ind. Int'l & Comp. L. Rev. 375

Slobogin C, Privacy at Risk : The New Government Surveillance and the Fourth Amendment (University of Chicago Press 2007) DOI: http://dx.doi.org/10.7208/chicago/9780226762944.001.0001

Slobogin C and Schumacher JE, 'Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society' (1993) 42 Duke L.J. 727

Solove D, 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 Stan. L. Rev. 1393
——, 'The Origins and Growth of Information Privacy Law' (2003) 748 PLI/PAT 29
——, 'A Brief History of Information Privacy Law' [2006] PROSKAUER ON PRIVACY, GWU Law School Public Law Research Paper No. 215 1
Solove D and Schwartz P, Information Privacy Law (3rd ed, Wolters Kluwer Law & Business; Aspen Publishers 2009)
Solove DJ, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' (2002) 75 Southern California Law Review 1083
Sun C, 'The European Union Privacy Directive and Its Impact on the U.S. Privacy Protection Policy: A Year 2003 Perspective' (2003) 2 Nw. J. Tech. & Intell. Prop. 99
Tzanou M, 'Data Protection in EU Law: An Analysis of the EU Legal Framework and the ECJ Jurisprudence' in Christina Akrivopoulou and Athanasios Psygkas (eds), Personal data privacy and protection in a surveillance era : technologies and practices (Information Science Reference 2011)
——, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88
Whitman JQ, 'Two Western Cultures of Privacy: Dignity versus Liberty' (2003) 113 Yale Law Journal 1151

How to cite this article: Maria Tzanou, 'The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?' (2015) 31(80) Utrecht Journal of International and European Law 87, DOI: http://dx.doi.org/10.5334/ujiel.cq

Published: 27 February 2015