Owe Langfeldt
o.langfeldt@googlemail.com

Securitization and Data Protection: The Case of the Passenger Name Record Agreements and Security Knowledge

Schriftliche Arbeit zur Erlangung des Akademischen Grades „Master“
an der Fakultät für Wirtschafts- und Sozialwissenschaften
der Eberhard Karls Universität Tübingen

Erstgutachter:
Prof. Dr. Thomas Diez

Zweitgutachter:
Dr. Thomas Nielebock

Tübingen, 22. Dezember 2010.

Table of Contents

Tables

List of abbreviations

API(S)	-	Advance Passenger Information (System)
ATS	-	Automated Targeting System
BATA	-	British Air Transport Association
CAPPS (II)	-	Computer Assisted Passenger Prescreening System (II)
CBP	-	Customs and Border Protection
CRS	-	Computerised Reservation System
DG	-	Director General
DHS	-	Department of Homeland Security
DPA	-	Data Protection Authority
ECJ	-	European Court of Justice
ELDT	-	European Liberal Democrat and Reform Party
EP	-	European Parliament
ESTA	-	Electronic System for Travel Authorization
GDS	-	Global Distribution System
JHA / JLS	-	Justice and Home Affairs / later renamed Justice, Liberty, Security
EDPS	-	European Data Protection Supervisor
ESTA	-	Electronic System for Travel Authorization
IATA	-	International Air Transport Association
ICAO	-	International Civil Aviation Organisation
MEP	-	Member of the European Parliament
PNR	-	Passenger Name Records
PPE-DE	-	European People's Party – European Democrats / Parti populaire européen – démocrats européens
PSE	-	European Socialist Party / Parti socialiste européen
TSA	-	Transportation Security Administration
VWP	-	Visa Waiver Program

1 Introduction

In the aftermath of 9/11, a plethora of measures to increase air transport security were enacted around the world. Organisations such as the International Civil Aviation Organization (ICAO) promulgated new standards and some states made unilateral changes, for example allowing armed "air marshals" on planes. Some of these new policies were uncontroversial, such as reinforcing cockpit doors; others caused heated discussions and diplomatic impasses. While there certainly are risks in aviation, perceptions differ a lot (Thomson et al. 2004), and there is no consensus on which remedies are to be chosen.

An especially contentious issue has been the transfer of Passenger Name Records (PNR) from the EU to the USA. PNR are records stored in airlines' booking systems and contain a lot of information about travellers – itineraries, credit card numbers or other payment information, special service requests such as kosher or halal meals, and so on. While initially collected for commercial purposes only, law enforcement and intelligence agencies became increasingly interested in them, and, after changing its aviation code in autumn 2001, the USA demanded this information from airlines flying to the USA. European data protection, on the other hand, legislation would have prohibited such a transfer without an explicit international agreement.[1] The airlines thus had to choose whose law to break, and to remedy this situation, an agreement was concluded in 2004 (EU-USA PNR Agreement 2004), only to be nullified by the European Court of Justice in 2006 due to formal mistakes in its legal foundation. After an interim period, a second short-term agreement was concluded in autumn 2006, before a new agreement was signed in 2007 (EU-USA PNR Agreement 2006; 2007). In the meantime, the USA pressed for and concluded bilateral agreements with several EU member states.[2] Similar agreements have been signed between the EU and Australia and Canada (Hobbing 2008). Some commentators decry an abandonment of core principles of EU law in these agreements (De Busser 2009), others point to the fact that the EU itself did not seem to

1 For a brief overview of EU privacy law see (Bennett and Raab 2006: 78-85).
2 Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, Slovakia (Hobbing 2008: 49).

take its avowed principles seriously (Mitsilegas 2008; Papakonstantinou and de Hert 2009).

This raises the question of "how come?" Although the aforementioned agreements with other states than the USA are closer to European law, neo-realist considerations of power do not help to understand this. Even with respect to the USA, the threat to deny landing rights to European airlines could have been easily reciprocated (Hobbing 2008: 27). They also cannot explain why the subsequent agreements came closer to American positions. On top of this, if the European Union really had not wanted such agreements, it would not have concluded them with the other states such as Canada and Australia, where negotiation leverage should have given it an advantage. Functionalist arguments do not improve our understanding of it either: While they may be able to explain why a functional spill-over effect may occur, they cannot tell us how the political debate on what to do about it will be decided (Huysmans 2006: 85-89). Additionally, assessments of PNR's utility are mixed – whether using them provides added value is questionable and questioned (see below section 2.1), thus further casting doubts on accounts of their use being a logical response to functional imperatives.

The argument I put forward is a different one. I argue that there has been a shift in the relationship between policy-makers and the professionals of security –the security bureaucracies of police agencies and secret services– which privileged the latter. Faced with their professional knowledge and the routinisation of data transfers, opposing policy-makers had a hard time arguing for other factors such as civil rights to be considered. The security professionals in turn crafted cooperation according to their own perspective, brushing aside such concerns. In the end, both the USA and the EU wanted to increase cooperation with one another (Mitsilegas 2008: 123). Framing the data transfer as a security issue both made it more urgent and precluded a more open debate. I argue that the relative influence of these two groups changed in the different rounds of negotiations, which is why the 2007 agreement allows for a wider range of uses for transferred data and longer retention periods – in those talks, the logic of security prevailed and became stronger than in the first rounds.

This argument is grounded in a connection between the Copenhagen and Paris Schools in security studies. Using the term "schools" in conjunction with their geographical origins is not meant to suggest inward-looking closed enterprises confined to specific places, but rather as a necessary means of ordering related approaches (van Munster 2007: 239-240). Other labels used to designate these approaches are securitisation theory and international political sociology, respectively. While these two approaches put forward related arguments, there are important differences (Bigo and Tsoukala 2008). Some even claim that there are only "minimal overlaps" (Peoples and Vaughan-Williams 2010: 70). Against this, I argue that the two can be fruitfully connected by using insights from the Paris School to better understand when and how securitizing moves can be successful. So where are these similarities and differences?

The Copenhagen School initially saw "security" as a speech act: By framing an issue as a security issue, it is elevated above "normal" politics and the normal rules of the game are suspended, because if it is not acted upon, "we will not exist to remedy our failure" (Buzan, Wæver, and De Wilde 1998: 26). Security is thus about existential threats to a referent object – be it the state, the economy, society or the environment, which in turn legitimise exceptional measures. Such securitising moves are negotiated between a securitising actor and an audience (Balzacq 2005). The question is what security *does*, not what it *is* (Buzan, Wæver, and De Wilde 1998: 26). While Buzan and his colleagues also list effects on inter-unit relations as part of securitisation processes (ibid), the Copenhagen School is – just like other discursive approaches – focused on agenda setting and discursive legitimation, less on implementation and the mundane details of bureaucratic politics (Huysmans 2006: 90).

This misses a big part of the story, as the Paris School argues. Started in the nineties by Didier Bigo (Bigo 1992; 1996), its roots lie more in political sociology and criminology than in international relations (Bigo 2008a: 126-127). As most of its early works have been published in French (e.g. Bigo 1992, 1996; all direct quotes my own translation), the Paris School was a latecomer to the English-speaking discussion, but by now it is a recognised approach in critical security studies (c.a.s.e. Collective 2006: 449). It focuses on the practical aspects, the technocratic face of police cooperation, and also re-

jects the claim that there is anything special about *international* security. From this point of view, "security" is less about the spectacle of exception but more about the everyday practices of "security professionals" as well as the effects of technological advances such as databases or surveillance at a distance and the struggles between different security agencies (Bigo and Tsoukala 2008). It focuses on the implementation and routinisation of policies and highlights continuities in policing: In the end, not that much changed post 9/11, many seemingly new trends can be traced back further in time (Huysmans 2006: 5-6; Bigo 2008b: 96). Implementation is not understood as a purely mechanical matter, either: Agents have considerable leeway (Huysmans 2006: 86; Bigo 2002: 72-73). When techniques are used frequently, they become routinised – what once was exceptional becomes the new normal. The Paris School's questions concern the professional knowledge of these agents and how their practices shape the securitisation of issues because "in technocratic or modern societies expert knowledge is inherently political" (Huysmans 2006: 10). "Shaping" hints another difference: securitisation is not understood as the outcome of purposeful action, but rather as a resultant of struggles within the field of security professionals, with each actor contributing to the process, but no single one dominating (Bigo and Tsoukala 2008).

While the Copenhagen School indeed misses the importance of technology (Huysmans 2006: 92), the approach of Bigo and associates has its blind spots, too. In the end both suffer from the same problem: They do not tell the whole story. The Copenhagen School ends too soon by neglecting the audience and by not elaborating on what using "exceptional measures" entails in practice. On the other hand, the Paris School starts too late by not clarifying how professionals of security's perceptions can shape the political agenda in the first place, even if control of the security apparatus is one of the core aims of the constitutional state (Loader and Walker 2007). Bridging the gap between agenda setting and legitimisation on the one side and implementation on the other in order to tell a fuller story is thus a worthwhile enterprise.

Such an undertaking must go beyond a simple statement that securitisation in the Copenhagen School's sense provides a window of opportunity for the professionals of security to take over the agenda. Such an argument neglects that the lines between "pro-

fessionals of politics" and "professionals of security" are not as clear-cut as they may seem at first glance. High-level police and secret service functionaries often are entrepreneurs for their respective institutions – and therefore have an agenda of their own – and often are political appointees. Their arguments and statements feed back into political discourse; the relationship is thus not a one-way-street: Just like professionals of politics enable professionals of security by providing them with new legal tools, the latter enable the former by providing them with talking points and professional knowledge. They depend on each other, one enabling and constraining the other and vice versa. What is interesting is how exactly they interact.

Examining this link is difficult due to the secretive nature of these agencies, but nevertheless possible. Finally, a sustainable synthesis of the two theoretical approaches also needs to take their epistemological and ontological compatibility into account. Since both share a broadly constructivist world-view, combining them is – although there are important differences in accentuation – easier than some of the other tasks to be accomplished.

Valuable work in this vein includes Jef Huysman's *Politics of Insecurity*, which introduced a shift towards implementation and the role of technology (Huysmans 2006: 86), as well as the c.a.s.e. Manifesto, which explores the connections between different critical approaches to security studies (c.a.s.e. collective 2006). An engagement with the criminological literature (e.g. Ericson 2007; Lyon 2001; Lyon 2008) on this issue might well add value. In fact, Ericson (2007) has already expressed similar ideas, although with a different vocabulary. Indeed, an interdisciplinary dialogue between international relations on one side and criminology and surveillance studies on the other is overdue (Bigo 2006a: 46; Sheptycki 2007; Aradau and van Munster 2009). Systematically connecting these two disciplines is beyond the scope of this work, though. Thus, I will only draw on criminological texts from time to time.

The contribution of this thesis to securitisation literature is twofold: On a theoretical level, it bridges the gap between two prominent approaches to security studies and thus provides a better understanding of the process of securitisation. In the empirical part, I will provide a study of an important part of international security cooperation. While the

PNR agreements have been mentioned in several articles, they have usually been examined from a bird's eye view (Bigo 2008b; Mitsilegas 2005, 2009), or from other – usually legal or normative – perspectives (De Busser 2009; González Fuster and de Hert 2007; Ntouvas 2007; Papakonstantinou and de Hert 2009). An in-depth study with an explicit theoretical framework is still missing.

The rest of the thesis will be structured as follows: First, a background chapter familiarises the reader with the facts and the development of passenger data exchange practices. After surveying the current literature on the subjects and pointing out its gaps, I will then present the theoretical frameworks of both the Copenhagen and Paris Schools. The theoretical presentation focuses on those aspects relevant to the topic at hand. Specifically, this means that while discussing the Copenhagen School regional security complexes will be omitted; for the Paris School, I will focus on the field of security professionals and the role of knowledge and practices. For both approaches, a discussion of their normative aspect will have to be left out. In a second step, I will then explore their connections and propose a connecting model for the two approaches. The following methodology section explains how to apply the model to the case at hand and discusses difficulties due to lack of access to documents and practitioners. With these theoretical foundations in mind it is time to start empirical work. The model developed before will be applied to trace the development and to provide a better understanding of how practices reached their current form. A concluding section sums up the findings and places them in the context of the ongoing renegotiations for new PNR agreements with the USA, Canada, and Australia. Finally, I suggest directions for future research and look at normative implications.

2 Background

This chapter provides background on the issue at hand. The first part presents an overview on what exactly PNR are, who collects and exchanges them with whom for which purposes. It also surveys the literature on their probable usefulness for law enforcement purposes. The second part outlines key facts about the development of USA-EU passenger data exchange – the 2004 agreement, the European Court of Justice (ECJ) decision of 2006, the 2006 interim agreement and the 2007 agreement.

2.1 PNR – Definition and Use

In the early days of aviation, tickets consisted of paper strips detailing each leg of the trip (for this paragraph, see Hobbing 2008: 2-11). As air traffic grew, this became impractical, and after some years of experimenting, the first computerised reservation system (CRS) which could be accessed from afar and stored this information in electronic PNR became operational in 1959. Today, all airlines operate such systems. Aside from this, there are global distribution systems (GDS) which allow booking tickets for a large number of different airlines. Some data fields are included in all PNR, others vary between different CRS and GDS (see ICAO 2004). PNR always contain the passenger's name, contact details of the travel agent, a ticket number, the itinerary, and the name of the person making the booking (ICAO 2004). Other fields may include remarks on requested services (vegetarian meals, wheelchairs etc.), hotel and car reservations and so on, leading to a length of up to 60 data fields (House of Lords 2007: 9). Some of the information may be stored in different systems called departure control systems, for example seating information (ICAO 2010). As PNR were intended for commercial use, standards for accuracy were lower than those which would have been required for law enforcement use (House of Lords 2008: 8) – mistakes in spelling could be corrected easily without adverse consequences to the traveller; however, when used for law enforcement purposes, mistakes could lead to mix-ups entailing false arrests. The table below lists information usually contained in PNR:

Data usually contained in PNR

Field	Content
Flight information	Airline, flight number, code sharing information[3], route, travel dates
Additional contact information	Home address, phone numbers, age information if needed (e.g. unaccompanied children, elderly passengers requiring assistance)
Frequent flier information	Frequent flier number
Payment Information	Credit card or bank account numbers, fare details, restrictions applying to the ticket
Other information	Special service requests (meal requirements, seating preferences), other service information (passed on to ground staff to assist passengers, e.g. wheelchair needed), changes to the PNR

Table 1: Data usually contained in PNR (compiled from ICAO 2010: 9-10; Hobbing 2008: 70-71)

These databases had originally been established for purely commercial reasons, large-scale use by law enforcement only began after 9/11, when US Customs and Border Protection (CBP) – as part of the newly-formed Department of Homeland Security (DHS) – was assigned the task of analysing them (Hailbronner, Papakonstantinou, and Kau 2008: 189). After the first wave of aircraft-related crime – the high-jackings of the early 1970s – reactions had focused on screening passengers for weapons and extradition agreements instead (Elias 2010: 2-12; Sweet 2009: 38-47).

The use of PNR should not be confused with Advance Passenger Information Systems (APIS), which also provide some information on travellers before they enter the country (ICAO 2004). The data included in these are mostly taken from the machine-readable parts of travel documents and comprise names, document number and expiry date, nationality, issuing country, date of birth, and gender (House of Lords 2007: 9). While this dataset contains less information than PNR, it is sufficient to check passengers against no-fly-lists. Unlike PNR, they have been created specifically for law enforcement purposes. APIS are used in programs such as the Visa Waiver Program (VWP) for visa-free travel to the USA and the Electronic System for Travel Authoriza-

3 Flights operated in cooperation by two airlines.

tion (ESTA), a program to clear passengers before they leave their home countries when travelling there (Hobbing 2008: 11, Elias 2010: 175-177). The European Union also implemented a similar program and demands API for flights entering its territory (Mitsilegas 2005: 2-7; Council of the European Union 2004b). Implementation rates are very low, however (House of Lords 2008: 12-13).

Whether PNR are actually useful is a contested matter. While there are frequent calls to analyse them, also within Europe (ORF Futurezone 2008; critical towards this: Article 29 Data Protection Working Party 2007a; European Data Protection Supervisor 2008), assessments with evidence for their expected usefulness are hard to find.

The airlines themselves are sceptical, as the British Air Transport Association (BATA) states: "[...] PNR data is so sketchy at times that it is of limited use to the authorities." (House of Lords 2007, evidence: 54). They might be useful, as the British House of Lords concluded in its inquiry into the issue (House of Lords 2007). However, the house also acknowledged that an over-reliance on PNR can have horrendous consequences, such as in the case of Maher Arar, a Canadian citizen, who was wrongly accused of Al Qaeda ties due to faulty interpretation of PNR. He was detained by US officials and later brought to Syria, where he was held and tortured for a year. A subsequent investigation made it clear that the allegations were completely insubstantial. The House also complained that witnesses examined for its report would not divulge details on investigations in which PNR had been useful, thus undermining democratic scrutiny. Even on an abstract level, witnesses could not name any cases in which PNR helped in terrorism investigations (House of Lords 2007: 9-13). The European Commission at first expressed similar frustration in its implementation meeting with DHS (European Commission 2005), but seemed to be convinced later (European Commission 2010b: 17). Data protection authorities are sceptical: "To date no evidence has been shown that data other than API data are necessary in the fight against terrorism and organised crime." (Article 29 Data Protection Working Party 2007a).

On their own, PNR may only be little "little though precious pearls" (Hobbing 2008: 53). Their use lies in the ability to link them to other resources – credit card numbers can lead to financial information, frequent flier numbers might uncover past trips and so

on (Hobbing 2008: 53-54). When stored for longer periods, they may help to uncover links between persons, for example when they use the same credit cards, or telephone numbers, or travel together (House of Lords 2008). However, basing decisions on such intelligence needs to take the accuracy of underlying databases into account (Elias 2010: 180). As pointed out above, the accuracy of PNR databases is sub-par. They could also be used for data mining, meaning the "extraction of meaningful intelligence, or knowledge, from the patterns that emerge within a database" (Gandy 2003: 28); however, such applications have been explicitly excluded by all EU-USA PNR agreements. The data may only be used to check travellers against a range of databases and targeting rules or in the course of criminal proceedings (Elias 2010: 177, also below 2.2).

Security agencies tend to be secretive about specific evidence for the added value of PNR analysis. DHS claims they are successful, but does not provide any numbers (Elias 2010: 177). Voices from within DHS have presented some anecdotal stories and make the claim that access to PNR data might even have stopped the 9/11 attacks, but still do not offer quantitative assessments of PNR's utility (Chertoff 2007; DHS 2007a; Baker 2010: 91-94). The UK Home office claims usefulness as well, focusing more on immigration matters. It also claims that PNR have been useful in fighting terrorism, but refuses to share information on that with the public or even the House of Lords European Union Committee (House of Lords 2008, evidence 13-14). The European Commission has also expressed frustration about not receiving reliable data on PNR's utility during the negotiations with the USA (House of Lords 2007, evidence: 40). Newer Commission documents assume usefulness, but do not offer statistical evidence for this assessment (European Commission 2010a: 3-4).

Nevertheless, several states pressed the issue and demanded PNR from incoming flights – Australia and Canada analyse PNR as well. The conclusion of the agreements and frequent news about plans to install a similar system within the EU show that they "are here to stay" (Papakonstantinou and de Hert 2009: 917). Using these records for law enforcement and intelligence purposes is compatible with broader trends in systems used for detecting terrorists and other criminals, moving from personal surveillance to monitoring data trails (Koc-Menard 2009). Summing up, the adaptation of PNR data for

law enforcement and intelligence purposes is a relatively recent phenomenon. Unlike API they were originally meant for commercial use which also makes it harder to use them for security purposes – the data organisation differs between different GDS, for example. Despite these difficulties security agencies press for an increased use of PNR. Evaluations of their utility are also part of the constructions analysed in the empirical part.

2.2 Development of USA-EU PNR Transfers

This section provides an overview of how the issue developed over time, starting with the run-up to the 2004 agreement and then covering the 2006 ECJ decision, the interim agreement, and the new agreement, which was concluded in 2007.

The immediate reason for the 2004 agreement was the Aviation And Transport Security Act of 19 November 2001 which stipulated that airlines offering flights to the USA provide PNR data to CBP "upon request", which was interpreted by the Administration to mean access to the airlines' CRS. Further rules were included in the Enhanced Border Security and Visa Entry Reform Act of 2002.

After these laws came into force, European airlines were essentially facing the choice whose law to break (Papakonstantinou and de Hert 2009: 899) because European privacy law banned transferring personal data to other jurisdictions that do not offer an "adequate", i.e. roughly comparable standard of of privacy protections. The EU informed the USA of this in June 2002 (European Commission 2003: 3). In general, the U.S. does not offer such protections (Bennett and Raab 2006: 83, 105). While CBP postponed the application of this law to European airlines, it would not completely waive the right to impose fines on them, and after the deadline for implementing the necessary technical changes to their booking systems passed on 5 March 2003, some large airlines started transferring the data. The Commission accepted this under the condition that negotiations for a full agreement were started (Papakonstantinou and de Hert 2009: 901; European Commission / US Customs 2003).

Negotiations began under the EU's first pillar and principal agreement was reached on 16 December 2003 (DHS 2003c). The final agreement was signed in Washington on 28 May 2004 (EU-USA PNR Agreement 2004). Just prior to this, on 14 May 2004, the Commission issued a decision declaring the provided level of data protection to be adequate, which was required for transferring personal data to a third state (European Commission 2004a). Annexed to this decision was a letter by DHS ("Undertakings") on the scope of data transfer and its intended uses. Earlier, data protection authorities (DPAs) had already criticized the planned scope of data transmission as being too wide (Article 29 Data Protection Working Party 2002; 2004a; 2004c).

As specified in the Undertakings, up to 34 data categories were to be transferred (for an overview of the categories and a comparison to the 2007 agreement see Hobbing 2008: 70-71). As only data fields actually collected by the airlines were to be transmitted, the usual extent was lower, averaging around 8 to 10 (airline spokesperson quoted in Council of the European Union 2006b: 5). This happened via a "pull" system, meaning that CBP could access airlines' booking systems to extract the data it needed. Under EU privacy law, a "push" system, in which airlines transfer the data themselves instead of giving CBP access to their data, would have been appropriate (Article 29 Data Protection Working Group 2003: 6). CBP was allowed use the data for "preventing and combating 1. terrorism and related crimes; 2. other serious crimes […] that are transnational in nature" (Annex to European Commission 2004a: 35). Forwarding them to third authorities (excluding transfers between CBP and the Transport Security Administration (TSA), but including other parts of DHS) was possible on a case-by-case basis only. Sharing them with third countries was not mentioned. According to the DHS Undertakings, data should be stored for 3.5 years, significantly less than the 50 years demanded at first (Bolkestein 2003a: 2). However, data transferred to other databases such as the Automated Targeting System[4] (ATS) or the Computer Assisted Pre-Screening System II (CAPPS II, see DHS 2004a; 2004b) were to be governed by the rules in place for them. In the case of ATS this initially meant a retention period of 40 years (Hobbing 2008: 43).

4 ATS is a system originally developed for threat assesments relating to inbound containers on ships, but later expanded to screen persons as well (American Civil Liberties Union 2007).

The only planned means of redress was an administrative procedure within CBP. The US Freedom of Information Act of 1966 and the Privacy Act of 1974 were technically applicable as well. However, the former includes several exceptions related to law enforcement use, while the latter is largely restricted to US citizens and legal residents. In the end, neither one provided sufficient rights to access and correct the data subject's own data, as demanded by EC privacy law (Hobbing 2008: 43-44).

On 27 July 2004, the European Parliament (EP) filed two lawsuits before the European Court of Justice attacking the Council and Commission decisions on which the agreement was based (EP 2004a; 2004b). On 30 May 2006, the court judged the agreement and the adequacy decision to be *ultra vires* because the first pillar was not the appropriate legal basis (European Court of Justice 2006). In the court's view, the legal basis had to be searched in what was the third pillar back then. The court did not examine the material merits of Parliament's complaints, since the agreement was declared invalid on purely formal grounds (for analyses of the judgement see Ntouvas 2007 and Guild and Brouwer 2006). The new agreement was to be negotiated in the third pillar without any substantial involvement of Parliament (Hobbing 2008: 45). Additionally, there was no general legal framework for data protection in the third pillar at that time, unlike in the first one.

The court allowed the nullified agreement to remain in force for a transitional period until the end of September 2006. This deadline seemed too strict for negotiating a completely new agreement, so an interim agreement was proposed (Papakonstantinou and de Hert 2009: 903-905). After intense negotiations it was signed in mid-October 2006 (EU-USA PNR Agreement 2006). For the period between the first agreement's lapsing and the signing of the second one, the EU agreed to let the transfer continue. The agreement itself remained largely unchanged compared to the first one, except that now additional authorities were allowed to use the data and they could be forwarded to Canada as well. For the details of the transfer, the Undertakings of 2004 remained in force. However, DHS also issued a side letter which significantly altered the terms of the Undertakings (reproduced in Council of the European Union 2006a, annex 3). According to the letter – which was officially annexed to the Council decision – the data could be shared

openly among all US agencies that undertook some counter-terrorism function or dealt with public health concerns. Moreover, the restriction to accessing only 34 out of up to 60 PNR data fields became indicative, and the retention period for data that had already been transferred could be extended without any oversight as long as the interim agreement remained in force. The agreement included a sunset clause for 31 July 2007 (Papakonstantinou and de Hert 2009: 906-907) as well as a clause according to which carriers should switch to a "push" system when the necessary technical changes had been made. Until summer 2007 only three European carriers had implemented a "push" system that fulfilled DHS's criteria (European Commission 2010b: 25).

A new agreement, which included a clause on provisional application pending ratification, was signed by the European side on 23 July and by the American side on 26 July 2007 for a period of seven years. However, national parliaments were slow to ratify (Papakonstantinou and de Hert 2009: 907). Now that the Lisbon treaty is in force, the European Parliament would have to give its assent as well, which it has not done yet and does not plan to do until the Commission has addressed some of its complaints about the use of PNR (European Parliament 2010: 2). The agreement is still applied on a provisional basis (Council of the European Union 2010). It consists of three parts: The agreement itself, which outlines the objectives, a letter by DHS in which it explains the way it wants to handle the data, and a letter by the EU acknowledging having received these assurances and considering them adequate. These two letters have been annexed to the Council decision and published in the EU's official journal (EU-USA PNR Agreement 2007).

Again, the substantial content of data is defined in DHS's letter, not the agreement itself. While both DHS and the EU touted a reduction in the amount of data transferred, this was misleading: Instead of 34 data *fields*, there are now 19 data *groups*, which each can contain more than one item – for example, the fields "travel agency" and "travel agent" have been merged. In the end, the maximum number of data items to be transmitted actually increased from 34 to 37 (Article 29 Data Protection Working Party 2007b: 9-10). The retention period was extended to seven years in an operational database and then 8 additional years in a "dormant" database which could only be accessed

with a senior DHS official's approval. How the data should be deleted is relegated to future discussions between the EU and the USA. It can now also be shared with third agencies in bulk (Hobbing 2008: 48). Which periods apply to data which has been forwarded to other agencies is not specified anywhere (Papakonstantinou and de Hert 2009). Instead of the earlier “pull” system in which DHS accessed airlines' booking systems the transfer is supposed to occur via a “push” system meaning that airlines themselves transmit the data to DHS, as soon as the technical prerequisites were in place. As of spring 2010, 15 European Carriers had such systems in place (European Commission 2010b: 25). Rights to redress were initially given in accordance to the 1974 Privacy Act – however, as most of its provisions only apply to US citizens and legal residents, they were not useful to European travellers.

Shortly after the agreement was signed, DHS also retracted the application of certain rights to access which had been granted under the Privacy Act (Hobbing 2008: 48). In total, the privacy safeguards provided were insufficient under European law (Article 29 Data Protection Working Party 2007b). Parallel to this, the USA concluded bilateral PNR agreements with several EU member states (Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, and Slovakia, see Hobbing 2008: 49) while ratification of the EU-USA PNR agreement was pending. In those negotiations the USA used its Visa Waiver Program as a bargaining chip – citizens of some EU member states still needed visa to travel the USA, a requirement that was waived after the conclusion of the agreements (Papakonstantinou and de Hert 2009: 917-919).

In summary, the scope, retention periods and possibilities of sharing transferred data increased, while rights to access and rectification barely changed, and if so, for the worse. The agreements are “thin” texts, with the actual amount of data to be transferred and its uses defined in unilateral side letters. Due to the change in the legal basis between the first and second agreement, the European Parliament had no formal competences during the negotiations for the latter agreements. Now it can give its assent, which it chose not to do (European Parliament 2010). The agreement has been provisionally applied for 3.5 years now, half of its duration.

3 Theory

This chapter is the heart of this thesis. First, I will review the literature on PNR and their exchange and address its shortcomings. The first and foremost of these is that there is an utter lack of theoretically informed case studies, which is a gap I intend to fill. In order to do so, I will then provide an overview of both the Copenhagen and Paris Schools. The goal is not to provide a complete history of both approaches, thus theoretical development will only be touched upon in passing: The focus is on providing a state of the art account for both theoretical lenses. A fourth subsection then discusses connections between both approaches to show that claims of "minimal overlap" (Peoples and Vaughan-Williams 2010: 70) are exaggerated. This section will also put forward a model to connect the two in order to better understand the dynamics of contemporary law enforcement and intelligence cooperation. A final section discusses the methodological framework for bringing this model to bear on the case at hand and the problems encountered in doing so.

3.1 State of the Art

The PNR agreements have been the subject of a number of reports, working papers and journal articles. However, when being covered in depth, they are usually approached at a rather descriptive level, or with a view towards legal and ethical implications. Those works that explicitly include a theoretical framework, on the other hand, tend to skim at the surface, with the agreements usually presented as just another example for increased surveillance of travellers or changes in the governance of borders. Seen from a different angle, PNR agreements can also be analysed within the literature on EU-US law enforcement cooperation. I argue that none of these can adequately explain how the agreements came about. In order to lead the way to my proposed answer to this lacuna, I then present current debates in critical security studies, which then lead to a closer examination of the Copenhagen and Paris Schools in the next two sections.

Some articles simply describe the content of the agreements (Guild 2007; Hailbronner, Papakonstantinou, and Kau 2008). A good overview is provided by Hobbing, whose main concern is the EU-Canada Agreement, although he also compares it to the EU-US

agreements to highlight differences (Hobbing 2008). The consequences of the ECJ's decision are further spelled out in other articles (Guild and Brouwer 2006; Ntouvas 2007). The conflict over their exchange has also been used as an example for the back-and-forth in the transatlantic relationship and increased cooperation in border control issues (Koslowski 2006). The question of transatlantic security relations in general is the topic of a rather diverse literature on its own (see for example Mahncke, Rees, and Thompson 2004; Freedman 2005; Forsberg and Herd 2006).

Other articles see the source of contention in different frameworks for privacy protections on both sides of the Atlantic (Tanaka et al. 2010) and understandings of the concept (Rees 2006: 116-117), which might even be traced back to different "cultures of privacy" (Whitman 2004). It is also argued that neither side had an adequate framework – on the European side, this was due to the lack of a unified data protection framework in the third pillar at the time the 2006 and 2007 agreements were signed (Papakonstantinou and de Hert 2009). Other legal discussions addressed the issue of how to ensure proportionality in the face of such deficient legal frameworks (González Fuster and de Hert 2007) and how the principle of purpose limitation, one of the core principles of European privacy law, has been weakened in the later agreements (De Busser 2009). Others discount these fears as overblown (Stentzel 2010). In a more general vein, the preconditions European human rights law – especially the European Court of Human Rights' case law – imposes on international data transfers have been analysed (Guild 2010). Related questions include the role of public-private partnerships in aviation security (Lahav 2008) and beyond – to which extent are, can, and should private actors be incorporated in the provision of security measures?

Other theoretically minded contributions see the agreements as yet another instantiation of the "(in)security continuum", an increasingly transnationalised field of increased surveillance of travellers and migrants (Mitsilegas 2005) and point to the role of technology (Balzacq 2008). However, they tend to take a bird's eye view, painting a picture of how the management of global human flows changed. This is even more true for works in the wider debate on the global visa regime (Amoore 2006; Salter 2006). The same applies to studies of surveillance beyond the state (Abrahamsen and Williams

2009), of which the use of PNR is presented as an example. A rare exception, although not specifically referring to the PNR agreements, analyses DHS's organisational discourses to arrive at a better understanding of its practices, arguing that these give a special ontological status to future disasters, seeing them as "[r]eal without being actual [...]", and thus focus strongly on perceived vulnerabilities (Martin and Simon 2008: 286). In surveillance studies, using PNR for security purposes is also seen as a further movement towards a "safety state" (Lyon 2006). This ties in with discussions on the role of risk and its management in governing today's societies (O'Malley 2006; Mythen and Walklate 2008; Dillon 2008). Here, Europe is seen on the forefront of adopting "risk" as a guiding principle (De Goede 2008).

The use of PNR for law-enforcement also raises questions of profiling: Heralded by its supporters as being more objective than prior techniques used by screeners, it is accused of hiding the same stereotypes under a mask of "scientific accuracy" (Curry 2002; Gandy 2006; Guzik 2009). Such techniques have also been introduced in the European Union with respect to money laundering and are under consideration for a planned PNR system for incoming flights (González Fuster, Gutwirth, and Ellyne 2010: 3-4). There is a strong belief in technological "fixes" in Europe (Guild, Carrera, and Balzacq 2008: 4).

From a different perspective, all this is also part of the research on police and intelligence cooperation, which generally claims that such cooperation is nothing new, although there some changes towards increased deployment of police abroad to be observed (Deflem 2002; Andreas and Nadelmann 2006). Within the EU, there is a proliferation of formal and informal networks between security officials (Bigo 1996; Gerspacher and Dupont 2007), and of information exchange (Müller-Wille 2008). Overviews of EU-US cooperation can be found in Aldrich 2004 and Kaunert 2007. Some claim that institutions and exchange agreements alone are not sufficient for improved cooperation, and that a common culture or identity of security agencies is needed to ensure efficient cooperation (Walsh 2006).

What has received only relatively little attention is the question of how and why the agreements actually came into being. At first, the answer seems simple: Transferring PNR was required by US domestic law, so Europe did not have a choice (Balzacq 2008:

91). While initially convincing, this cannot explain why the subsequent agreements moved closer to American positions. If this was about the USA imposing her will on a reluctant EU, then why did plans for analysing PNR appear there as well (see e.g. Home Affairs Commissioner Franco Frattini in EP 2007d)? Why did EU negotiators agree to expand sharing and retention of transferred data? Why did they also enter into agreements with Canada and Australia, where negotiation leverage should have favoured their side, if they supposedly were wary of PNR transfers as a matter of principle? Or was it the case that both sides wanted to increase cooperation, including exchange of information on travellers (Mitsilegas 2008)? Even if the US was the one to start such initiatives, they seemed to fall on fertile ground in Europe (Mitsilegas 2009).

Summing up, there is a quite diverse literature on the issue of using PNR for law enforcement purposes. Yet the question of "how come?" is still unresolved. How exactly can we make sense of why the agreements came about and how do we understand the subsequent changes? My attempt to do this is grounded a connection between the Copenhagen and Paris Schools of security studies. The first is an important part of the "discursive turn" in the discipline, while the second contributes to the less prominent "practice turn". Previous attempts at connecting these two are Huysmans' (2006) account of migration in Europe, Salter's (2008a) study of aviation security in Canada, with van Munster (2007) pointing out questions for the further development of critical approaches to security.

Huysmans criticises discursive approaches to security for neglecting the role of technocratic politics and security professionals and proposes a "foucauldian view on spillover" in which their knowledge constitutes a "regime of truth" framing what can be said and done about security issues (Huysmans 2006: 85-104). Not discounting the drama which is often part of security politics, he sees a bifurcation of politics into spectacle on the one and routine on the other hand (Huysmans 2006: 153-155).

Salter (2008a) uses dramaturgical analysis inspired by Erving Goffman's work to study how securitising moves are played out and justified towards different audiences. He suggests four different settings in which securitising moves can occur: Popular, elite, technocratic, and scientific settings, each with its own grammar and standards of proof.

The different rules of the game in each of these settings reflect their actors' habitus, establishing a connection to thoughts associated with the Paris School.

Van Munster in turn rightly points out three unresolved tensions within critical approaches to security, two of which are relevant to my enterprise here (van Munster 2007): First, the question of authority – who can speak or do security? That is to say, is "security" constructed by the public discourses of politicians, or is it a matter of bureaucratic struggles, routinisation and technology? Second, what is the role of the exception? Is security about exception, or about routinisation, or could it be said that the exception is the new routine? These two questions are important because the Copenhagen and Paris Schools' respective answers to them diverge. Reconciling them is then a part of the theoretical labour to be done in formulating an integrated approach. But first it is time to examine both approaches in greater detail.

3.2 Copenhagen School

One common answer to the "how come"-question would be that the issue has been securitized, here meaning that something is proclaimed to be an existential threat to a referent object, which in turn justifies exceptional measures – for our case: Terrorists using air travel in order to carry out attacks or just enter the country threaten the well-being of travellers and transportation security. Therefore, considerations of privacy are not applicable here, as the unfettered exchange and analysis of information must take precedence to protect the public, including strong threats such as revoking landing rights for non-compliant airlines.

This logic of securitisation is the main contribution of the Copenhagen School of security studies. The name was coined by McSweeney in an article criticising early contributions to this line of thought (McSweeney 1996). A different label would be "securitisation studies"; I prefer to stick with the geographical moniker because the term securitisation is also used by the Paris School, albeit with different content. The Copenhagen School is not about what *security* is or is not, but what it means to address issues as security issues. The main question can be phrased as "who can 'do' security in the name of what?" (Buzan, Wæver, and De Wilde 1998: 45), which implies a move away from tra-

ditional security studies (as exemplified by Walt 1991). “Who?” is a question which was not foregrounded in traditional security studies – it was deemed obvious that security was done by and about states. Instead, the Copenhagen School argues that other actors can also “do” security. “Doing” security means that “security” is not a concept which is “out there” and has a fixed content – instead, it is a linguistic practice. When obeying certain rules, actors can invoke “security” to lift an issue above normal politics. This is the core of the Copenhagen School: By securitizing issues, the constraints of normal politics are removed and they are dealt with as a matter of urgency, reminiscent of Carl Schmitt's thoughts on the state of exception (Williams 2003: 517-21). “In the name of what” points to a third move: While traditional security studies privileged the state in its military role as referent object, this opens the field for other referent objects – economy, environment, society, the political system.

The concept of securitisation is the Copenhagen School's most influential contribution. As it is the most relevant for my purposes here, I will focus on it in the following section. Other parts of the theory, such as regional security complexes (Buzan and Wæver 2003), its normative stance (see Behnke 2000; Huysmans 2002), and macrosecuritisations (Buzan and Wæver 2009), will be left out because they are not relevant to the case at hand. Before going into greater detail on how who can securitise what under which circumstances, a few remarks on ontology and methodology are in order.

The Copenhagen School subscribes to a constructivist ontology and and a discours analytic methodology, which in terms of ontology this means that “social relations are not laws of nature but the contingent product of human action” (Buzan, Wæver, and De Wilde 1998: 204). Compared to more critical scholars who emphasize their malleability, these constructions are seen as rather stable, as “sedimented” (ibid: 35). This means that while they are in principle constructed, they can be taken as given when working on specific cases – “inert constructivism”, so to speak (ibid: 205). Its goals are a better understanding and managing of relations, rather than emancipation, which has sparked a lively debate on the normative implications of security research (Eriksson 1999; Behnke 2000; Huysmans 2002). In terms of methodology, the Copenhagen School uses a discourse analytic approach.

Buzan, Wæver, and De Wilde (1998) claimed that applied to "security" this constructivist ontology means that the concept is self-referential: It is by addressing issues as security issues that they become such; the concept has no fixed content, there is no "essence" of security. Tanks crossing a border are no security threat in themselves – they may take part in a joint manoeuvre or a peacekeeping operation. The task is thus not to find out whether threats "really" endanger a referent object, but to study these processes of securitisation, in which the features of the threat invoked may play a role, but only as "facilitating conditions" (Buzan, Wæver, and De Wilde 1998: 32). While its contents may vary, the form is fixed (Williams 2003: 516): An issue is presented as an existential threat to a certain referent object which in turn justifies emergency measures. [5] However, there are some inconsistencies here: Seeing "security" as self-referential discounts the role of the audience – security can be self-referential or intersubjective, but not both (Balzacq 2005: 177; Stritzel 2007). I will return to this later.

This takes us right into the heart of the matter: How does securitisation work? As outlined above, a securitizing actor frames an issue as an existential threat to a referent object. Besides these, there are functional actors which influence the process without being either the securitiser or referent object. This first step is called a securitizing move; it is only after this move has been accepted by the relevant audience that an issue becomes securitized. Each of these terms will be explained in greater detail below.

Securitising actors can take diverse forms. Traditionally, they have been state officials, but other groups – lobby groups, environmentalists and so on – can make securitizing moves as well, depending on their capacity to organize (Hansen 2000). In the end, high-level politicians and state officials frequently have an advantage since the audience usually assumes that they have access to better information, "[s]ecurity is thus very much a structured field in which some actors are placed in positions of power by virtue of being generally accepted voices of security [...]" (Buzan, Wæver, and De Wilde 1998: 31). On top of this, the aforementioned sedimentation of social practices comes into

5 Ironically, this can be seen to imply statements about what "real" security problems are, i.e. those that are about survival and that actors who talk about security in other contexts just get it wrong (Ciută 2009: 307, 320-321). This contradicts claims that the Copenhagen School is agnostic as to whether something is a "real" threat and that "security is what actors make of it" (Buzan, Wæver, and De Wilde 1998: 35). Ciută admits, however, that empirically most conceptions of security conform to this model.

play: because security has traditionally been about the state, state officials are in a privileged trusted position when it comes to defining threats (ibid: 37; Balzacq 2005: 190-191). While individuals do the actual talking, they are only speaking in their roles on behalf of organisations: "France-materialized-as-de-Gaulle rather than the Person de Gaulle"; this "methodological collectivism" means that collectivities such as states can be seen as more than just the sum of their members (Buzan, Wæver, and De Wilde 1998: 40-41). It is important to note that this is not meant to be an a priori privileging of state actors, although it is sometimes construed that way (e.g. by Barthwal-Datta 2009): They just happen to be the most frequent securitising actors. Although they are not exclusive wielders of the authority to securitise, they are the usual suspects.

In terms of referent objects, the Copenhagen School shares the widening agenda (for a discussion of this body of work, see Buzan 1997). Who or what is constructed as being threatened may vary – both in terms of sectors and of levels. Buzan and his colleagues identified five sectors of security: Military, political, societal, economic and environmental. In each of these, constructed threats take different but related forms. There are different levels of referent objects as well: units such as states or nations, subsystemic regions (example: European identity vis-à-vis immigration), or even the whole system (example: a possible nuclear conflict during the Cold War as a threat to the international system as such). However, the individual is excluded as a referent object. Theoretically, "securiziting actors can attempt to construct anything as a referent object" (Buzan, Wæver, and De Wilde 1998: 36). Empirically most securitized referent objects are found on the unit level – e.g. states or nations. Securitising actor and referent object can be the same, e.g. a state (ibid: 36-40). Indeed, this was implicitly assumed in traditional security studies. In our case, the referent object would be American national security including the ability to manage borders and protect its own citizens when using aeroplanes.

Functional actors, in turn, are a concept which has not received the attention it deserves. These are actors who influence the dynamics in a sector while being neither securitising actors nor referent objects (ibid: 36). The example given is that of a polluting company in the securitisation of environmental issues. Functional actors may launch

counter-discourses as said company would do, but they can also serve as a reservoir for claims made by securitising actors, e.g. in appeals to scientific or professional authority. This concept remained underspecified so far; it seems to be a catch-all term for everything else that may be important. Functional actors may influence the audience in deciding whether to accept the securitising move, or be a kind of an audience in themselves – for example a bureaucracy that needs to go along with a move to give it momentum. In the sense that they form the background against which a securitising move is played, they offer an interesting possibility for a linkage with thoughts about the role of the field and prior discourses which figure prominently in the Paris School. How exactly this plays out will be elaborated in section 3.4.

Framing an issue – any issue – as an existential threat to a designated referent object is the central part of a securitizing move. By putting an issue in terms of survival, it is elevated above normal politics: "If we do not tackle this problem, everything else will be irrelevant (because we will not be here or will not be free to deal with it in our own way)", and this is why exceptional measures need to be taken (Buzan, Wæver, and De Wilde 1998: 24). The initial concept of a "speech act" claimed that in saying something, it is done (Austin 1977). Austin named four conditions for a successful speech act: There must exist a *conventional procedure* which is *fully executed* in a *sincere way* and fulfilled in that *actors conduct themselves according to the procedure* (Balzacq 2005: 174-176). A promise or naming a child could be examples, and an issue becomes a security issue by being addressed as one using the "security grammar" of existential threat, urgency, and call for extraordinary action – irrespective of whether there is a "real" threat or not. The word "security" does not necessarily have to be uttered; the concept can be used in an implicit manner. In some domains it is also understood that when we talk about "this", we talk about security – e.g. defence; what matters is not the word "security" but the claim of an existential threat (Buzan, Wæver, and De Wilde 1998: 24-27). However, what exactly has to be present in the absence of the word "security" has not been spelled out yet (Buzan and Hansen 2009: 216). This is an important gap: If analysts can decide whether something constitutes implicit usage of the concept

"security" independent from what the actors themselves say, then security is not what actors make of it, but what analysts make of it (Ciută 2009: 303).

Furthermore, this formulation of security as a speech act downplays the role of the audience and hints at a cleavage within the Copenhagen School as to how exactly "security" should be conceptualized as a (linguistic) practice and as to what affects a securitizing move's likelihood for success. There are two "centres of gravity" in it, one stressing the importance of adhering to the grammar of security, and the other focussing on external conditions such as the "fit" between a securitizing move and established discourses in the audience (Stritzel 2007: 359). This is the tension between a self-referential and a dialogical conceptualisation of "security" mentioned above. These two different points of view have been dubbed the "internalist" and the "externalist" strand (ibid). Both sides further elaborated the grammar of security by breaking it down into its individual steps (see Balzacq 2005, 2009 for the externalist side and Vuori 2008 for the internalist one).

I side with the externalist strand because it pays greater attention to the audience's role and to facilitating factors for a securitizing move's success. I also follow Balzacq (2005: 173) in that securitisation should be seen as a strategic practice, not as a speech act. As Buzan, Wæver, and De Wilde acknowledge, securitisation can have a tactical appeal for policymakers (1998: 29). In convincing the audience, however, sincerity, one of Austin's conditions for a speech act is routinely violated. Secondly, seeing it as a speech exaggerates its formality – unlike pronouncing a marriage, its success is not determined by adherence to the rules, it depends on context (Balzacq 2005: 174-176).[6] Taking this externalist view has three advantages: Firstly, it allows us to focus more on studying how and when securitizing moves are successful. The second advantage is that by loosening the focus on speech as such, images and bodily performances can be included more easily (as urged by Hansen 2000: 302; see also Williams 2003: 524-528; Balzacq 2005: 178). This externalist understanding can also provide a better role for functional actors. If we want to study *processes* of securitisation, these functional actors have to be

6 Another point: Balzacq argues that seeing "security" as a speech act takes one part – illocution (doing something *in* saying something – in our context, claiming an existential threat) – for the whole situation, which also includes perlocution (the intended effect of the speech act – in our context, acceptance by the audience) (2005: 177).

taken into account as well: Take Buzan, Wæver, and De Wilde's example for a functional actor, a polluting company in the environmental sector; instead of standing idly by the sidelines, it would try to influence the securitisation process by launching its own discourse to influence the audience.

What has been discussed so far were the ingredients for a securitizing move. To move to a full securitisation, the "relevant audience" has to consent to the framing suggested by the securitizing actor. Accepting the securitising move does not have to happen in a "civilized, dominance-free discussion" (Buzan, Wæver, and De Wilde 1998: 23), but nevertheless, there is some need to argue, the audience cannot just be coerced. It can also resist them and thus the success of securitizing moves is never guaranteed (ibid: 25-26, 31). An initially neglected concept, the audience is central to understanding securitisation. If security sits "among" the subjects, as Buzan, Wæver, and De Wilde said (1998: 31), then to whom precisely do securitizing actors talk? Two questions are important here: Who is relevant and how do they make up their minds, i.e. which factors influence the likelihood of a securitizing move being successful?

Initially, two conditions were named: Adherence to the four rules of the speech act as outlined above and "external, social conditions", most notably holding a position from which such claims can be made. However, despite their insistence that "successful securitization is […] decided by the audience" (ibid: 31-32), its role remained underspecified.

Who the relevant audience is depends on the political system and the issue at hand. Initially developed for more or less democratic systems, the model can be adapted to non-democratic settings as well; there, the relevant audience usually is the power elite (Vuori 2008). Even in democratic systems, the relevant audience need not be the general public: One suggestion has been to distinguish between formal and moral support (Balzacq 2005: 184-186). "Moral" means support by a target population (e.g. supporters of majority factions in parliament). It is not a sufficient condition though, since in the end it is the formal support by an institution – most often the legislature – that brings about emergency measures. While strictly speaking formal support is sufficient, some securitizing actors tend to be responsive to the wider audience's opinions – after all,

members of parliament want to be re-elected. However, this is not enough. Before an issue reaches the parliamentary floor, it has usually been discussed in bureaucratic administrative settings. Additionally, as Salter (2008a) has pointed out, different kinds of audiences are receptive to different kinds of arguments – bureaucracy, science and politics work according to different logics. What counts as a good argument in one of these settings may be ineffectual in another. Securitisation within professional circles can serve as a reservoir for legitimacy for securitising moves in the political sphere via the appeal to to technocratic or scientific authority. While this may be a contributing factor for success, it is not sufficient. Take climate change for example: Within scientific circles it has been understood as an existential threat since almost to decades while a securitisation in the political sphere has arguably not occurred until today (Salter 2008a: 325).

Just saying that a securitizing move's chance of success depends on "a variety of contextual, institutional, and symbolic resources for its effectiveness" (Williams 2003: 526) is not enough, either. So what makes successful securitizing moves more likely? Combining Stritzel's (2007), Balzacq's (2005, 2009), Salter's (2008a) and Williams' (2003) suggestions, the following influences can be distilled:

- Audience: Does the argument made to justify the securitising move resonate with discourses already present in the audience? Does the audience consider the securitising actor to be trustworthy and knowledgeable, taking into account the specific standards of proof required by that audience? Can the audience grant a formal mandate?
- Context: How is the argument presented? Which role do other media, such as images, play?
- Securitising actor: Is the frame of reference tailored to the audience? Is the actor in a socially accepted position to define threats (positional power)?

These contextual factors influence whether a securitizing move is likely to be accepted or not. Summing up, the theoretical model as reconstructed here can be visualized as follows, with lightning depicting possible venues of influence for functional actors:

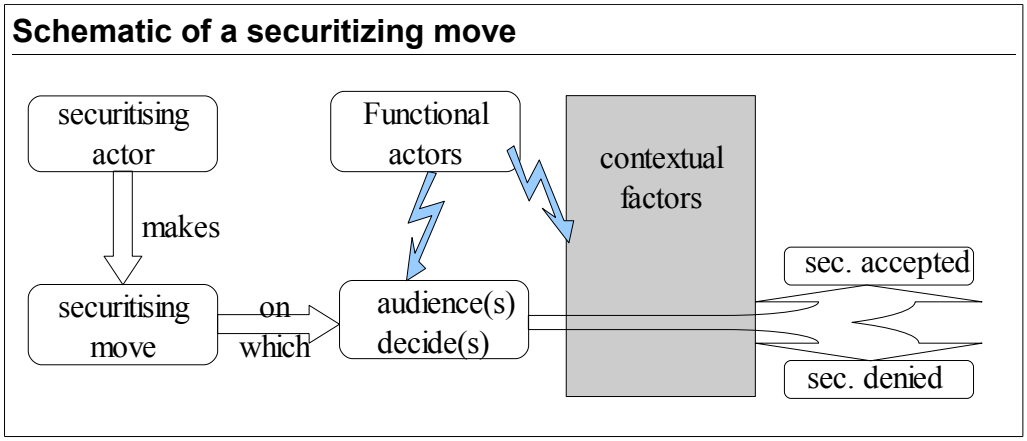

Table 2: Schematic of a securitising move

Compared to the initial suggestion by Buzan, Wæver and de Wilde, this modified understanding of securitisation places greater emphasis on context conditions as opposed to the actual performative speech act. As shown above, the tension between these two aspects was present in Copenhagen School writings from the beginning. These theoretical moves to include context led away from understanding "security" as a speech acts towards making sense of it as a practice. However, these contextual factors still give the impression of acting as stopgaps. The grey box's placement does not fully do them justice: While they influence the audience's decision, some of them are properties of securitising or functional actors themselves or the relations between them: Whether a securitising actor is considered trustworthy or not is not just a property of that actor, it is derived from a wider social context and past interactions which define who may speak in the first place. Furthermore, once a securitisation has been successful, it constitutes the new status quo, endowing the securitising actor with new powers and discursive resources. The actors are embedded in a social field. How this embedding influences them is a main focus of the Paris School to be examined in the next sub-chapter.

Returning to the case at hand, one could suspect that appealing to 9/11 to justify the use of PNR might have become less convincing over time, because the subsequent attacks in Madrid, London, and elsewhere did not use aircraft as a means of attack. If these logics of exception still work way they did shortly after 9/11 – and it is safe to say they do – then there is more to it than the Copenhagen School sees. Here, the Paris School can provide further insights into how securitising moves are embedded into a

discursive field. What also remains under-theorized is what happens after a securitizing move has been accepted by the audience. Is its implementation a purely technical matter, or do the tools used affect the way problems are dealt with? Or, more provocatively: Can tools themselves securitise an issue to the point that an audience's assent is not really needed any more (see Balzacq 2008)? After all, issues often slip under the public's radar when framed as purely technical questions. Are bureaucracies which implement policies just executive organs or do they have an influence of their own? This leads to a line of thought associated with the Paris School: The roles of technology and of the bureaucracies which implement security policies on a daily basis. This embedding of securitising moves will be the subject of the next section.

3.3 Paris School

From the Paris School's point of view, the narrative seems to be different. Using this approach, one would argue that an increasingly transnationalised field of security professionals united by a common habitus managed to gain hold of the negotiations and thus sidelined other actors such as the European Parliament. Using their professional knowledge, they saw value in exploiting PNR for intelligence and law enforcement purposes, something which united them in spite of bureaucratic battles for turf, legitimacy, and budget – and sitting on different sides of the Atlantic. This line of reasoning can help to understand why the 2007 agreement imposed fewer restrictions on using the data. In these negotiations, Europe was formally represented by the then German Minister of the Interior Wolfgang Schäuble, who headed the Justice and Home Affairs Council at the time, assisted by the Commission's JLS directorate. As will be shown in the empirical chapter, they – unlike the Commission's internal market directorate, which headed the 2004 negotiations – shared DHS's view of the world to a considerable extent which explains the relatively smooth negotiations in this round.

This first sketch introduced the Paris School's key terms and concepts: *Security professionals*, their *practices*, *knowledge*, and *habitus*, the *field* they form, and the role of *technology*. Each of these will be explained in detail below, but first I will outline this approach's ontological and methodological assumptions. According to the Paris School,

what kind of world do we live in nowadays? What is to be understood under the label "security", how is it related to the exception, and what are important developments? And, last but not least, how do we find out about them?

Like the Copenhagen School, the Paris School's conceptualisation of "security" is discursive. However, there are more explicit links to post-structuralist theory, especially drawing on Michel Foucault (Buzan and Hansen 2009: 219). One important thought is that "knowledge" itself is constructed. What can be defined as a "security" issue is thus not dependent on some kind of external yardstick of what "real" threats are. The security agencies themselves are the main site of production for this kind of knowledge. Instead of just being tools implementing policies defined by the legislature, they play an important role: By their understandings of the "threat" and the – usually technical – means to fight it, they construct a space of what can be said about "security" and thus shape policy responses. As the ones in charge of actually controlling borders and policing crime, they are seen as competent authorities on the subject, which gives them leverage in arguing for new powers (Huysmans 2006: 10). Staying true to its post-structuralist background, the Paris School abstains from claims on whether these threats are actually true. To the contrary, it is argued that by producing truths about their adversaries – for example via statistics – claiming dangers emanating from them, they produce their own subject (Bigo 1996: 54-55; Bigo 2000: 195; Salter 2008c).

Who are these objects of insecurity? Traditionally, they were clearly defined: Police dealt with an internal adversary, the criminal, while the military had an outside enemy. These clear borders are becoming more and more blurred by constructing new threats such as migrants and terrorists who are neither here nor there. The metaphor used here is the Möbius ribbon – it is not clear whether one is on the inside or the outside, one is both at the same time and yet neither (Bigo 2002: 63). While such developments have been under way for quite some time, the end of the Cold War accelerated them, because it necessitated a redefinition of the roles of many security agencies, as their old enemies disappeared and new adversaries were needed to maintain budgets and legitimacy. One of these new enemies is "the migrant" (Huysmans 2006), terrorists are another one. Addressing these "new threats" is claimed to require more resources and competences for

security agencies, securing their budgets and turfs, as well as increased international co-operation.

Unlike securitising moves in the Copenhagen School's understanding, these processes of redefinition are creeping, securitisation – a term that is used here as well – is seen as being about routines: "Some (in)securitization moves conducted by the bureaucracies or private agents are so embedded in these routines that they are never discussed and presented as exceptions." (Bigo 2008a: 128). While some of the extra-ordinary measures may initially be accompanied by the drama associated with securitising moves in the Copenhagen School's understanding, they become routine in the long run – biometric passports and telecommunication data retention are examples. The explicit invocation of the exception as understood by the Copenhagen School's Schmittian roots is not the usual way securitisations come about. For example, only the USA and to a limited extent the UK officially declared an exception after 9/11 (Bigo 2006: 47-48), which led Bigo to conclude that the "normalization of emergency as a technique of government by unease" and the practices of security professionals are what matters (Bigo 2006: 53, 63). In this sense, practices are understood as the "profound structure" behind the moment of exception (Bigo 2006: 47). The claim is that by ignoring all this in favour of that final moment, the Copenhagen School misses the conditions which make such securitisations possible in the first place (Bigo 2002: 73). These practices also mask the belief in technological fixes (Bigo 2006: 49): There is a widespread assumption among the professionals of security (more on them below) that technological means of surveillance via databases can "fix" the problems identified, be they fraudulent asylum seekers, undocumented migrants, or, in our case, terrorists on aeroplanes. The belief is not debated, it is taken for granted with looking to technology for fixes being a default reaction (Salter 2008c; De Goede 2008a; Bigo 2008b: 104-106; Guild, Carrera, and Balzacq 2008) Reliance on technology shapes the form of police work–it becomes less like using force on a person, and more like a bank managing credit (Bigo 2002: 75).

Summing up, constructed knowledge has the potential to widen the realm of security in a double sense: On the one hand, more issues are subsumed under the label of "secur-

ity", and on the other hand, security agencies cooperate more across borders. These supposedly "new challenges" lead to a blurring of the inside/outside distinction, which has an impact both on the self-understanding of security professionals and the field they form. This knowledge is constructed in the routine workings of the security agencies, thus the analytical focus is on their practices.

Next, turning to methodology: How do we find out about these practices? Which methods are used? As pointed out above, the understanding of security is discursive, with "discourse" understood in a wide manner; it is not only about words, but also practices. In embracing the "practice turn" the Paris School maintains that just studying public or elite discourses is not enough. One has to study how the agents involved actually do what they do: "To analyse these processes fully requires spending time with the people of the agencies, understanding how and why they use these techniques, and their legitimation of the routines of coercion, control and surveillance" (Bigo 2000: 176). Where you sit is not only where you stand, as the famous saying has it, "where you sit is what you *do*" (Pouliot 2010: 35, emphasis in original). This practice turn draws heavily from other disciplines, such as ethnology in its wish to uncover actors' perceptions and self-understandings, and sociology, from which it adapted concepts like Bourdieu's field (more on this later). The reasoning behind this methodological choice is that just focusing on official discourse runs the danger of reproducing it. Instead, researchers must aim to recover the dispositifs of the agents involved. Another term taken from Foucault's work, a dispositif is a wider notion than discourse: besides discourse both of the public and scientific variety, it also includes architecture, regulatory decisions, and administrative measures (Bigo 2008c: 43).

Using this approach calls for participant observation as a research method. Gaining this kind of access to security agencies is difficult, though, which is why most works in this line of research rely on qualitative interviews and the analysis of discourse as it is embodied in official documents, speeches, and other public statements, supplemented by analysing the relations between the different agencies (for a mapping of European security agencies, see CHALLENGE 2007). In conclusion, the Paris School's methodo-

logical tools usually usually are in-depth interviews and discourse analysis, since participant observation is rarely possible.

Turning to more practical questions, who are the security professionals, what do they do (and how)? What to make of terms such as habitus or field? These questions will be explored in the next subsection.

Moving beyond the Copenhagen School's study of security as a linguistic practice the Paris School examines the routines, perceptions, and professional knowledge of those "professionals of security" who "do" security – police agencies, border guards, intelligence services, security experts, and others (Bigo 2006: 31-32) – as well as the networks and the competition between them. These agents construct and try to monopolize knowledge about what can be defined as a security issue and how to address it, including technical means (c.a.s.e. Collective 2006: 457).

To tell whether a specific actor belongs to this field or not, the deciding criterion is not the real possibility of using force, but "the ability of the agents to produce statements on unease and present solutions to facilitate the management of unease" (Bigo 2006: 22). It thus not only includes police and intelligence agencies, but also some politicians, academic security experts, parts of the press, think tanks specializing in security issues, police unions, and so on (Bigo 2006: 30-31). In fact, the borders between these categories can be fluent. Stressing that what matters is the ability to make claims about security points to the importance of professional knowledge. There is a belief – both inside and outside the field – that "they" know things "we" do not (Bigo 2002: 74). In fact, similar statements are made in the Copenhagen School from time to time (Buzan, Wæver, and De Wilde 1998: 31). This can lead practitioners to nonchalantly claim that their ideas constitute common sense among those who know – "Surely this approach to border security is obvious." (Baker 2010: 25), precluding debate with the lay public. This "regime of truth" shapes what can be said in debates.

This knowledge is intertwined with the habitus of security professionals. Consistent with the focus on practices, this concept – borrowed from Bourdieu – refers to a system of durable dispositions that help persons to make sense of their surroundings by provid-

ing a matrix of perception, appreciation, and action (Pouliot 2010: 31). Four aspects have to be mentioned (see ibid 2010: 31-33, Bigo 2002: 73-78 for the following):

1) Habitus is historical, meaning that it is the sedimented consequence of past practices. It turns them into second nature, instilling path dependency in social interactions. This understanding of "how things are done" is instilled via socialisation, imitation, exposure and symbolic power relationships. In our case, being a police officer includes a lot of practices that are not consciously adopted but rather emulated from colleagues and superiors during work.

2) It is practical. Habitus cannot be learned from a book, it is acquired by long-term exposure to practices. It is also largely unarticulated: When asked why they do things the way they do them, people are often at loss for words – habitus is self-evident, it is "the way things are done". This is not to say that conscious thoughts do not play a role, but it is against a backdrop of unconscious knowledge that they do. In this sense, "being" a security professional is more than possessing technical knowledge, it is about a sense of the game, "the way things are".

3) Habitus is relational. The dispositions it entails are not individual in the sense that they stem from the individual herself; rather, they are social, shaped by past interactions. It is in this sense that habitus connects structure and agency.

4) It is dispositional. It does not force actors to mechanically do certain things, but it inclines them to do so. This differentiates it both from habit, which just repeats past patterns, and also from conceptions of a complete free will, because actors think and act within the bounds of their practical knowledge. In our case this means that professionals of security can of course question whether increased surveillance "works", but they are inclined to give it the benefit of doubt.

A shared habitus in turn creates a feeling of commonality – "[...] a cop is a cop no matter whose badge is worn" (Andreas and Nadelmann 2006: 232). Persons sharing a certain habitus can recognise each other at first sight and identify each other as "one of us" (see Bigo 1996: 51). This understanding of a shared "sense of the game" (Bigo 2002: 75) is remarkably similar to how Baker described then EU JHA Commissioner

Franco Frattini and then German Interior Minister Wolfgang Schäuble (Baker 2010: 134, 141). However, there are some methodological problems in analysing habitus and practices: As they are not explicitly mentioned and vocalised, on the one hand they must be at partly native to analysts so they can understand them; on the other hand, they must also be partly alien to them so that they don't stay invisible as second nature. If they are completely alien to the analyst, however, there would be an increased potential for misunderstandings (Pouliot 2010: 51). Summing up, habitus is a grammar for generating practices (ibid: 33). In itself, it is not sufficient to study practices, it is in relation to a *field* that we can use this concept.

The field is another concept based on Bourdieu and refers to a relatively autonomous social configuration of actors with its own internal struggles and rules (Bigo 1996: 49-56). Bigo and his colleagues initially adapted it for studying the relationships between law enforcement agencies in Europe. Applying this concept is still a niche enterprise in International Relations, as opposed to sociology, where it is widely used.

Fields can gain certain amounts of autonomy, just like the field of security did (Bigo 2002: 75). This means that they control their subject – in our case the management of fear – to such a degree that the actors in it can be sure that their claims about its subject cannot be easily manipulated from the outside. Pointing out that terrorism is a rather negligible risk from an outside position is not going to change perceptions inside the field. This field of security blurs formerly clear-cut decisions between the inside and the outside (Bigo 2006: 23-33). In this field, there is cooperation as well as struggle, but one thing is always true: Knowledge is power (c.a.s.e. Collective 2006: 457). Those actors who are accepted as being able to define what threats are to be addressed with which means have a lot of influence on shaping the course of policy. However, due to the multiplicity of actors in this field, no single one of them can purposefully securitise an issue on her own. To be more specific, the field of security is characterised by four aspects:

1) The field as a *field of forces*: There is a certain homogeneity among actors in the field; their bureaucratic interests are similar, they share ways of defining the potential enemy and of gathering knowledge about her. These perceptions are not identical, but still related. To localise specific actors in this field, one has to look at their professional

socialization and their positions of authority as spokespersons of "legitimate" institutions, that is, whether they possess the relevant social capital (Bigo 2006: 22-23). In our case, this means access to intelligence and capabilities to analyse it; see Chertoff's plan to improve DHS's standing in the intelligence community: "By having more to contribute [...] we will have frankly more vigorous place at the table." (DHS 2005h).

2) The field as a *field of struggles*: It is precisely *because* actors within it share similar perceptions of what is at stake that there are struggles between them (Bigo 2006: 23-25). They fight over budgets, missions and legitimacy. This idea is related to works on bureaucratic and small-group decision-making (e.g. Allison and Zelikow 1999; Hudson 2007). As pointed out above, it goes beyond them by taking the constructed nature of knowledge into account – their struggles are also about how to make sense of the issue.[7] To use the words of a practitioner: "Arriving at a single U.S. position for international talks is in itself a major negotiation." (Baker 2010: 110).

3) In relation to other fields, the field of security can act as a *field of domination*, meaning that the professionals of security monopolize the power to define what to fear (Bigo 2006: 25-27). This is where they can clash with professionals of politics. As their professional knowledge shapes their understanding of threats and how to respond to them (Huysmans 2006: 8), they enter into struggles with actors from other fields over how to understand issues. While some issues – such as their day-to-day work– are clearly within their own domain, there are "indeterminate spaces" where actors are "obliged to negotiate" with each other (Bigo 2006: 26). This is an area which will be talked about in more detail in the next section. The change in the style of negotiations between the 2004 and the 2007 agreements is instructive here. When negotiations were chaired by the commission, DHS faced stiffer opposition to its demands than it did in the subsequent rounds (Baker 2010:112). The council presidencies and the Commission's JHA directorate were closer to DHS than the Internal Market directorate.

4) The field of security is a *transversal field*: It fuses formerly separate social spheres, its borders are not fixed, it can change its shape (Bigo 2006: 27-33) – for ex-

7 See for example (Sales 2002: 304-312) for a description of such struggles in the context of secret service reform in the USA.

ample, when immigration was put on the security agenda, new agencies became part of the security field (Bigo 2002). Its borders are the results of struggles. Seeing the field of security as a transversal field allows us to study the interactions of security professionals beyond the state without enclosing the realm of investigation again by reference to a geographical unit such as "Europe". Finally, one could argue that there is a transnational field of homeland security.

Summing up, a field describes a set of related actors which share a common sense of the game, but are also bound up in bureaucratic struggles over turf and legitimacy. In this tangle, no single actor can move an issue onto the security agenda on her own. This is an important difference to the rather actor-centric Copenhagen School and should be kept in mind when combining the two approaches.

Another important aspect is the role of technology. Advances in information technology, sensors and other fields have opened up new possibilities for policing (Bigo 2002). Exploiting PNR for intelligence – which on today's scale would not have been possible 30 years ago – is just one example among many. So how exactly does technology enable and reinforce some of the tendencies outlined above?

Closing down borders in times of crisis – as the US did for the first few days after 9/11 – has long been a well-established "ritual of fear" (Bigo 2006: 52) when responding to unforeseen events. In an increasingly interconnected world it is not a viable option for the longer term, so with the help of technology, the focus of control changed: From fortifying borders to managing the populations crossing them (Bigo 2007: 10). This was made possible by advances in technology. It is the driving force here: It is not the case that new technologies are developed because there is a demand for them, but the other way around: What is available will be used (Bigo 2002: 73). Sometimes this involves adapting existing technologies to new uses: After the cold war ended, radar systems originally designed to spot Soviet missiles were being advertised as means to stop small planes used by drug smugglers (Andreas and Nadelmann 2006: 159). This increasing reliance on technology for "policing at a distance" (Bigo 1996: 13) then leads to calls for more technology where less has failed (Ericson 2007: 12). In the end, when all you have is a hammer, the world gets reframed as a nail (Bigo 2006: 55-56). The

hammers in question are systems for data mining and other surveillance technologies. Possessing such technical means is part of the social capital that helps actors to define their position in the field of forces.

To conclude, what is the Paris School's claim in a nutshell? Securitisation is the resultant of bureaucratic struggles and regimes of truth, not of a purposeful move by a single actor. These struggles occur in a transversal field of forces, struggles, and domination. Technology has been an enabler for this. Together with a shift in the policing of borders – from controlling and closing them to managing flows across them – it has facilitated an extension of security logics to new issues. Based in a belief in the possibility to manage them via technical means, this has lead to a proliferation of international data exchanges and networks. Often decried for civil liberties violations, these practices are accompanying the Schmittian exception with smaller, everyday exceptions (Buzan and Hansen 2009: 249-250). This embedding in routines makes practices initially regarded as exceptional look banal and normalises them in the long run.

This account provides a sociological understanding of how securitisations come about, but some problems remain. According to the Paris School, securitisation processes are slow and creeping. However, when looking at the real world, we see that some of the most important securitisation processes – while definitely based in practices and routines – rely on the public drama of the exception as understood by the Copenhagen School. As such moves are sometimes launched without being steeped in the routines, they are not mere epiphenomena of the "profound structure" of practices (as claimed by Bigo 2006: 47). The Paris School seems to neglect purposeful agency here: While it is certainly true that routines serve as enabling factors for Copenhagen-style securitising moves, there still is agency involved.

This leaves us with a problem: Both approaches offer a better understanding of some processes, but neither one tells the whole story. If the professionals of security depend on the professionals of politics to a certain degree, because bigger changes usually require parliamentary or at least top-level executive approval, and the professionals of politics depend on security professionals as a source of legitimacy, then it becomes clear that both parts are needed: Creeping processes provide a reservoir of justifications for

securitising moves in the Copenhagen School's sense, while the drama of the exception serves as a catalyst for securitisation processes as understood by the Paris School. They are two sides of the same coin. The next task is to connect them.

3.4 Bridging the gap

At first sight, the two approaches might seem rather remote from each other – on the one side we have a parsimonious adaptation of speech act theory to security studies that emphasizes the performative quality of elite discourse; on the other side, there is an approach grounded in sociology which looks into the details of everyday implementation and the role of professional knowledge. However, some of the theoretical enhancements made to better embed discourse in the Copenhagen School move it closer to the Paris School's outlook (Salter 2008a). Calling this a convergence of the two approaches would be to exaggerate the similarities, but the contributions by Williams, Balzacq, Stritzel, and Salter on the role of contextual factors influencing the likely success of securitizing moves point to a development which opens up the the formalistic speech act approach to a sociological study of professional discourses and knowledge. Further exploring these connections and proposing a connecting model is the task at hand for this section. In order to do so, I will first provide an overview of similarities and differences between the two approaches. The similarities identified there and attempts to bridge the differences will then form the basis for an integrated model. The following table provides an overview of key differences and similarities:

Overview of common ground and differences

Aspect	Copenhagen School	Paris School
Theoretical roots	Austin, Schmitt, Classical Realism	Foucault, Bourdieu
Ontology	"inert" Constructivism	Constructivism, closer to Poststructuralism
Security as...	Exceptional practice / speech act	Normalised practice, institutionalized routine
Where?	International	Blurred: internal-international
What can be securitized?	Anything	Anything
Role of the exception	Beyond politics	Exceptionalism inside liberalism

Overview of common ground and differences		
Aspect	**Copenhagen School**	**Paris School**
Who?	Open, usually politicians	Professionals of security, for the most part state officials
Agency?	Securitising actor facing an audience	Less important, securitisation as resultant of bureaucratic struggles
How?	Securitizing move via a performative act with an audience's assent	Institutionalization of a field of security professionals creating a regime of truth
When?	Specific point in time	Creeping process
Methodology	Discourse analysis	Discourse analysis, qualitative interviews, network analysis

Table 3: Overview of common ground and differences

Both approaches eschew an essentialist definition of security and look at how securitisation removes issues from the "normal" political agenda. The fact that both schools have distinct theoretical roots does not stop us from connecting them. As outlined above, at least a part of the Copenhagen School lessened the focus on speech acts and moved towards a deeper embedding of discourses. A lack of embedding has been a common criticism levelled against discursive approaches to security (Huysmans 2006: 91). The additions by Williams, Balzacq, Stritzel, and Salter were important steps to improve this embedding. Further elaborating on how securitizing moves are embedded in institutional structures and the discourses of the professionals of security can improve this even further. On the other hand, the Paris School stems primarily from Bourdieu's analysis of fields, coupled with a Foucauldian view on the construction of knowledge. This allows for a) a wider understanding of "discourse" to include non-verbal practices as well and b) for a thicker description of social practices.

Whereas the Copenhagen School at first talked exclusively about international security (Buzan, Wæver, and De Wilde 1998: 21), the Paris School claims that a blurring of inside and outside is one of the most important empirical developments in the real world and reserves a place for it in theory as well (Bigo 2002: 63). Copenhagen's exclusive focus on international security has diminished over time, with its securitisation framework also being applied to domestic issues (see e.g. Huysmans and Buonfino 2008; Salter 2008; Volpi 2007). Secondly, the insistence on being about international se-

curity only served as a way of distinguishing the approach from questions of social security. To give an example that the borders between internal and external can be blurry in the Copenhagen School as well: Suppose a societal group tries to securitise the presence of an ethnic minority as a threat to national identity with the governments of the state and that of the minority's home state as functional actors – this is neither purely internal nor external. It is obvious that although such a blurring is not explicitly mentioned, it does not contradict the framework. Therefore, this is no impediment to connecting the two approaches.

Both approaches – now – agree that in theory anything can be securitized (Bigo 2008: 124-125). What differs is the role of context: According to the Copenhagen School, professionals of politics are relatively free in which issues to (try to) securitise and security bureaucracies are largely left out of the picture. The Paris Schools in turn claims tight limits on the former's independent ability to frame issues. Nevertheless, these thoughts can be connected: If "to study securitization is to study the power politics of a concept" (Buzan, Wæver, and De Wilde 1998: 31), then it is not a big step to the "field of struggles" as described by Bigo (2006: 23-24). The connection between speech act and social context can be made clear picking up the example for a speech act mentioned above: Naming a child is a speech act without which the child would not have a name. However, registering or baptizing said child implies a set of institutionalized conventions. Once it is officially registered, the child cannot change its name at will. And without this set of conventions, the act of naming a child would remain inconsequential (Huysmans 2006: 24). Similarly, securitizing moves are usually embedded in a web of social practices which give meaning to them.

Looking at those social practices together with the "power politics of a concept" leads to the question of authority. Who is in a position of authority, how do they get there and how do they influence securitising processes? This does not only apply to securitising actors, but also to functional ones, to use the Copenhagen School's terms – the latter may intervene in debates to strengthen or weaken the former. This compels us to loosen the focus on the former, in order to see wider processes of how issues become security issues. It is not about brute power, or about formal positions, it is about the au-

thority to claim “security”. These are not necessarily correlated. It is possible, to imagine a situation in which police services have become discredited as enunciators of security claims, for example in states with an authoritarian past. Power is to be understood as the power to define what works and what needs to be done. This connects to the role of social capital. In our area of inquiry this means that the professionals of security are not only a possible reservoir for justifications by the professionals of politics for their securitising moves. They might start their own securitising moves, either overtly by claiming security threats in the public realm, or behind the scenes by lobbying professionals of politics.

Seen from the first point of view – security professionals' discourses as a reservoir of legitimacy for securitising moves – they become supporting actors in the play. Drawing upon their professional discourses can help to bolster legitimacy for securitising moves; as mentioned above, there is a presumption that “they” know things “we” don't. So if “they” agree, that is usually seen as a good reason by the audience. This view is still close to the more socially embedded strands of the Copenhagen School (see also van Munster 2007: 238 for a similar view on links between different texts). Professionals of security are seen as providing talking points and justifications for political actors here.

In the second mechanism, they take centre-stage and act as securitising actors in the Copenhagen School's sense. Here, it is interesting to study how discourses are appropriated, mobilised, or defused (van Munster 2007: 240). How do security professionals react to competing discourses, e.g. mounted by civil liberties groups or opposing politicians? Are they ignored, reframed, or even appropriated – once described as liberty coming back wearing security's clothes (Bigo 2008b)?

The third mechanism consists in lobbying and briefing professionals of politics and sharing “inside knowledge” with them. This strategy may be hard to observe if done discreetly. On the other hand, references made to them in justifying proposals for new powers, budget increases, or the use of new technologies can help to uncover these processes. Here, it is obvious how adding insights from field theory can help to improve the analysis: The Copenhagen School would treat the professionals of security as functional

actors, which would not do their role justice. In the Parisian framework, on the other hand, this is easily understood as a move to improve their own position in the field.

This shows that subsuming them under the label of "functional actors" does not really work. Sometimes they may serve as a discursive resource, fitting under that label, sometimes they also become securitising actors in their own right. This means that there is more to securitisation than the triad of securitising actor – securitising move – audience. The concept of field can help here. By embedding securitising moves in a wider social context, it becomes clearer which discursive resources are drawn upon and how these serve as a source of authority. Professionals of politics speaking security draw upon discourses already established in the audience and the field of security professionals. Nevertheless, one should not reduce securitisations to these background conditions, for the decision to securitise is still an eminently political choice (Williams 2003: 520-521). Seen this way, professionals of security depend on professionals of politics, too. The latter are the ones who authorize new powers for them, in the end.

Studying professional knowledge and field effects can thus add to analyses of securitisation processes by providing a better understanding of the context in which they take place. Studying the relationship between these two fields can then help to uncover the positional power of actors to find out who can speak security effectively by drawing on existing discourses (Williams 2003: 512).

The next question is how to reconcile the different understandings of the exception. To recall, the Copenhagen School argued that successful securitisations include breaking free of the normal rules, whereas the Paris School holds that the routinisation of "security" is what matters. How can this gap be bridged? In the end, it is not as wide as it might seem at first sight.

Although one of the Copenhagen School's roots lies in Schmitt's thoughts on the exception, the exception as understood by it does not require a wholesale suspension of the rule of law and the possibility of violence, as Schmitt had it. Instead breaking free of rules that would otherwise bind is the threshold for the exception (Buzan, Wæver, and De Wilde 1998: 25). This falls short of Schmitt's criteria by far. Fast-track legislation, heightened secrecy and a closure of public debate are sufficient (ibid: 27-29). Likewise,

the drama usually associated with the rhetoric of exceptional threats does not need to be constantly present – it can be implicitly understood that "when we talk about *this*" we talk about security (ibd: 27, emphasis in original). Securitisations can become sedimented, so to speak. Such sedimented securitisations are just as absent from public debates as the bureaucratic processes the Paris School focuses on. Over time, they become "normal" – almost no-one in Germany would question the Basic Law's emergency powers today, but when they were introduced in the late sixties, they caused a big stir. This is just what the Paris Schools means by "exceptionalism inside liberalism" (Bigo and Tsoukala 2008). Going further, some even argue that exceptionalism has become the new normal (Neocleous 2006; Basaran 2008), that it is included in the way everyday life is governed (van Munster 2007: 241). The difference lies in the role of dramatic invocations of the exception when items are removed from the normal political agenda – when they have become sedimented, there is no visible distinction. Whether they have been removed from "above" via dramatic exceptionalism or from "below" via routinisation does not matter in the long run.

So, in the light of the discussion above, how can the two approaches be reconciled? Going further than Hansen, who embedded security talk in context by showing how texts are linked (Hansen 2006), I aim at embedding discourses in their social contexts: The field helps in understanding who may speak with authority; looking at inter-agency relationships in there can also elucidate how actors shape their arguments differently based on the different audiences they might face. In this way, it is a double embedding in existing discourses and in bureaucratic conflicts.

These existing discourses can become normalised and self-justifying over time, providing ample possibilities to draw upon them in arguing for new security measures. They can also silence divergent views. Bureaucratic conflicts over turf, budgets, and legitimacy compel security professionals to engage the political sphere to improve their own position. So far, this is largely similar to the arguments put forward by the Paris School: Discourses and practices in the field of security professionals shape what can be said and done about security. However, these background conditions may be necessary, but they are not sufficient for securitisation to occur. This is where thoughts taken from

the Copenhagen School come back in: While their likelihood of success is largely contingent on these sedimented background conditions, there is an unavoidable element of agency here, as outlined in the three mechanisms presented above. Someone has to seize the opportunities. This is the element that is missing in the Parisian approach: While it details the underlying conditions of possibilities for securitising moves, it fails to explain how the final step comes about and how it works. This is where the Copenhagen approach can help. Its focus on audiences and justificatory strategies can help to see interventions that seek to upset the established ways of practice and routinisation that might get swept away by the rather technocratic outlook of the Paris School (van Munster 2007: 240).

So in the end, both are needed to understand securitising processes in greater detail: The regime of truth as constructed by the professionals of security serves as the conceptual backdrop against which political moves of securitisation are played out. Then again, the professionals of security cannot expand their legal powers on their own; for this, they need political approval by an audience. This audience need not be the general public, as evidenced by the US military's "black programs" (Buzan, Wæver, and De Wilde 1998: 28). So while they play an important role in delineating what *can* be said, they do not enjoy an as important role in actually *saying* it. This is not to discount their importance in this arena, but just to point out that they have to share this arena with the professionals of politics, scholars, and civil society. In this sense, my argument offers a more socially embedded view of securitisation than the Copenhagen School does, but does not discount possible resistance from other settings, as the Paris School sometimes does. This tendency, which once lead Bigo to assert that "[...] it is always administrative power that wins and procedures of public deliberation that are defeated" (Bigo 2002: 83), downplays the essentially political nature of securitising moves. In avoiding both Copenhagen's lack of attention to social context and Paris' fatalism as concerns the outcome of security politics, I hope to open new ways for inquiry into "security". The next question is thus how this approach can be put into use for practical research.

3.5 Methodology

Just like the approach presented here is a combination of the Paris and Copenhagen schools, its methods are quite similar to theirs. While the Copenhagen school uses discourse analytic techniques on policy-makers' statements, the Paris Schools also adds interviews with and observation of security professionals to its methodological tools. In this section I will first explain how my approach should be put into practice methodologically, before presenting the second-best model used for the actual research. This divergence is explained by the difficulties involved in getting access to the professionals of security's world. Because the best tools were not available, I had to fall back on discourse analysis. I go on to describe the corpus of text used for the analysis before concluding with reflections on its limitations.

In a –from researcher's viewpoint– ideal world a combination of ethnographic methods, expert interviews and discourse analysis could be used. The respective strengths of some of these methods would alleviate the weaknesses of others and vice versa.

Starting closest to the practitioners' experiences, participant observation could provide close scrutiny of how they actually go about their work and how they make sense of the issues at hand. This kind of "deep hanging out" (Pouliot 2010: 66-68) is chiefly inspired by Harold Garfinkel's works on ethnomethodology (Garfinkel 1967). While this method is well-suited for uncovering actors' routines, it suffers from some problems as well. For one thing, making sense of their actions requires a certain supply of background knowledge, which in turn needs to be problematised, similar to the problems in analysing habitus that I pointed out above (ten Have 2002: 34-38). For obvious reasons, using this method was not possible in this study.

The second part of the methodological tool kit would be semi-structured or narrative interviews. These can help to find out about how people in the field perceive the debates and what they think of other actors. In contrast to standardised interviews in which each interviewee is asked the same questions, these are a lot more open. Instead of a fixed list of questions, they use only a short number of guiding questions – after all, the task is to get the interviewee to talk.

The third part would be to analyse the organisational discourses in the field. A lot of divergent approaches are grouped under the label “discourse analysis” (Wodak 2008: 4-5). These range from relatively positivist approaches which use word counts as a quantitative tool to trace the development of discursive tropes over time, to post-structuralist accounts of self and other (see for example Hansen 2006). The understanding of discourse analysis espoused here falls in between these two extremes. The focus will be set on intertextual links – who quotes whom? – and tropes and justifications – which moves are made to convince which audience(s)?

Finally, triangulation combines the respective strengths of these techniques and alleviates their weaknesses (Wodak 2008). By taking insights from different methods of data gathering – for example expert interviews and analysis of public discourse – researchers can both avoid being lured into uncritically accepting actors' self-understanding and taking a too abstract view, discounting the practitioners' experiences. This would be what Pouliot (2010: 52-91) has called a “sobjective” methodology, a portmanteau of “subjective” – understood as being close to the practitioners and their understandings of the world – and “objective”.

While such ambitious research strategies are promising in theory, it is hard to put them into practice. Sadly, access to security agencies is limited: Not all relevant documents are made public, officials are reluctant towards interviews and even if they agree to be interviewed, they are still bound by restrictions on which information may be divulged to external researchers. Nevertheless, interviews are the best way to gain hold of the information needed, especially for insight into attitudes and the actual implementation of procedures which may be quite different from what is on the books. Within the scope of a master's thesis it is not possible to conduct the many interviews needed to get a comprehensive overview of practitioners' attitudes and beliefs, due to time and budget constraints. For comparison, Gerspacher and Dupont (2007) conducted their interviews over the course of several years, Bigo's seminal study draws on about a hundred interviews (Bigo 1996: 27), Pouliot conducted close to seventy interviews (Pouliot 2010: 84). I contacted several officials involved in the negotiations, but only one of them agreed to be interviewed. Statements from this interview are used as anecdotal evidence.

Since the best methods are not available due to the reasons outlined above, a second-best solution needs to be found. Further complications are added by the fact that many negotiation documents remain confidential, as agreed upon by the parties (Council of the European Union 2007). The analysis therefore has to rely on public statements by involved decision-makers and those documents which are public – either published by the institutions, or retrieved with freedom of information requests.

Documents published by the European institutions were retrieved via their respective websites or publicly accessible document management systems using the search term "PNR". When only the titles were publicly available, I filed document access requests. After examining them, the respective bodies provided me with 32 out of 65 requested documents, of which 2 contained redactions. For European Parliament debates, I ran a full-text search of the entire archive with the same search string. Council documents were less easily available, as it and DHS decided that negotiation documents should remain confidential afterwards (Council of the European Union 2007). DHS documents were searched by manually checking the titles of DHS press releases and other publications, including speeches and statements by officials. They also included several op-eds by senior figures which were published in newspapers. For DHS, I surveyed the releases until the end of 2007.

An initial screening weeded out documents that only contained corrections, administrative notices, forwarded documents by one of the other bodies, or were otherwise unrelated. Then, additional documents by the institutions already mentioned have been retrieved via a snowball method – i.e. documents that were referred to in the initial sample, for example reports of European Parliament committees and hearings of DHS officials in the US Senate and House of Representatives. Additionally to these documents, the hearings conducted by the House of Lords (2007, 2008) provided valuable insights with witnesses from the UK Home Ministry, the European Parliament and the Commission. The relative length of text devoted to discussions of these materials in the empirical part will not necessarily reflect the sheer numbers. Instead, I chose the texts to be discussed in more depth so as to convey an overview of the divergent views in the

debate to reconcile the conflicting aims of comprehensiveness and depth via selective sampling (Oberhuber and Krzyzanowski 2008: 189).

In the end, there are clear limitations on the usefulness of the data collected and the inferences which can be drawn from it. The lack of "closer" sources providing an inside view means that I might miss the important minutiae of what went on behind closed doors; this in turn heightens the risk of just reproducing official discourses and the justifications offered in it. What can be done to alleviate these concerns? Within the sources available, I will pay more attention and accord greater weight to free-form speech, such as in hearings, parliamentary debates, and so on. Compared to more vetted committee reports and press releases, these less scripted interactions provide a better perspective into how the persons involved make sense of the issue, as they may caught off guard or deviate from prescribed terminology. Seen this way, the House of Lords and European Parliament hearings offer a lot more information than just the factual content of the statements: How witnesses react to questions provides valuable insights into their understanding of the issue. While evidently not as well-suited for uncovering normally non-vocalised parts of habitus and personal attitudes as one-on-one in-depth interviews, these are as close as possible to this ideal under the restrictions imposed by the lack of personal access to the relevant persons. Taking these caveats into account, what shall we look for in the empirical analysis?

- Securitising moves, framing an issue as an existential threat that needs to be addressed immediately.
- References to professionals of security and their knowledge, be it in forms of statistics, criminalistic knowledge, anecdotal evidence or other forms of discourse. In general, justifications of proposed measures: Are arguments given, is their utility just assumed?
- Links in the other direction, with professionals of security championing certain political ideas and intervening in the debate on their own behalf.

– Lastly, the role of technology should not be neglected. How did the technological implementation evolve? Does it reflect changes in the debate, the other way around, or does it stay untouched by them?

As outlined above, the ideal methodological framework for this approach would be to triangulate using participant observation, interviews, and discourse analysis. However, using such an approach is not possible here, due to lack of access and space. This leaves us with using discourse analysis as a second or rather third-best solution. While deplorable, not much can be done about this. This imposes limitations as to how valid the following analysis may be. In this light, the following should more be seen as a plausibility probe than a full case study. Notwithstanding the given limitations, I am confident that useful knowledge can be gathered. With these caveats in mind, let us now proceed to the empirical part.

4 Applying the framework

This chapter applies the approach presented above to the empirical case. The subdivisions follow the development over time: From the first demands of the USA to the 2004 agreement, its nullification in 2006, on to the renegotiations leading to the 2007 agreement. Each of these subsections starts with the American justification and then presents the European side before talking about the technical implementation and summing up the findings.

4.1 The 2004 Agreement

One of the first legislative reactions to 9/11 on the American side was the Aviation And Transport Security Act 2001, which, among other things, mandated that PNR data for incoming flights be supplied. In the Senate and House debates on the bill, this measure was uncontroversial; in fact, it was not addressed at all in the floor debates – the contentious issues were the federalisation of of security controls at airports and current problems in passenger screening at the airports (US Senate 2001; US House of Representatives 2001a; 2001b). The law itself did not specify any purpose for the use of the data, or how it should be used.

Around the same time, the "wall" between law enforcement and intelligence officials was largely torn down. Traditionally, these functions had been separated and information flows between them were tightly controlled. One of the lessons drawn from 9/11 in the intelligence community was that these flows had to be deregulated (Baker 2003). Later, this was also echoed in the 9/11 Commission's recommendations (9/11 Commission 2004). DHS set out to work with the EU to get "[...] even more information, passenger name records, so we can better identify potential problems, individuals, that may have terrorist connections before they come into the country" (DHS 2003b).

Both before and after the agreement's conclusion, US officials defended their demands and the final results as an indispensable measure for fighting terrorists. In the words of Secretary of Homeland Security Tom Ridge, terrorism was "the new totalitarian threat" to be defeated, as a part of this fight "[...] this agreement will allow homeland security officials to protect America against terrorism and other trans-national threats [...]" (DHS 2004g). According to him, PNR were needed "[...] so we can better identify potential problems, individuals, that may have terrorist connections before they come into the country" (DHS 2003b). This assessment was echoed by James Loy (Deputy Secretary of Homeland Security) when speaking in Brussels: "It is an essential security measure that allows us to link information about known terrorists and serious criminals to co-conspirators and others involved in their plots." (Department of Homeland Security 2004e).

At the same time, Loy maintained that "[a]ll of the additional security capabilities that we are building have not, will not, and cannot ever come at the expense of our fundamental values or individual liberties." (Department of Homeland Security 2004e). When announcing the agreement's signing Secretary Ridge also claimed that the U.S. and the EU were "[...] equally committed to not only improving the safety of air passengers and the security of our borders, but also to protecting the privacy of air passengers consistent with both U.S. and European laws." (DHS 2004d), which had been arrived at after "hard-nosed" negotiations (DHS 2004g). In Ridge's words, while "[f]ear of government abuse of information is understandable [...] we cannot let it stop us from doing what is right and responsible." (quoted in DHS 2003a). When the EU's adequacy de-

cision was signed in May 2004, Ridge stressed both security and privacy as important values (DHS 2004c). After the agreement was concluded, DHS did not stop in pushing forwards, because, as Ridge said "[...] we can't allow whatever achievements or success that we've seen to this point to lull us into any kind of complacency or lose our sense of urgency." (DHS 2004g).

Summing up its position, the USA saw PNR data as an essential tool for finding out about terrorists before they entered the country and placed high hopes in their utility to uncover unknown connections between them. At least publicly, no evidence has been offered for these claims, usefulness was assumed. In public, there were no links in the other direction with law-enforcement officials championing the idea. The US slightly scaled back its initial demands, and was at least partly responsive to European demands for shorter retention periods and better data protection.

How did the EU react to these demands? As there were more debates on this side of the Atlantic, the presentation will follow the development over time, with special attention to the debates surrounding the EU - U.S. Customs joint declaration of February 2003, the principal agreement in December 2003, and the adequacy decision of May 2004.

After the Commission informed the US that a legal basis would be needed for the transfer in summer 2002, the issue was first discussed at a working level, with several parts of the Commission involved in the talks: Internal Market and Taxation, Transport, External Relations, and Justice and Home Affairs. Tensions between them caused the European Parliament to urge the Commission "to ensure genuine cooperation" between the different commissioners (EP 2003c). In the end, the matter was principally assigned to the Internal Market Commissariat, because this was where privacy expertise was located, and Commissioner Frits Bolkestein took the lead (Interview with a Commission official, November 2010).

The first to address the issue publicly was the Article 29 Group, the working group of the member states' Privacy Commissioners. It opposed any kind of US access, arguing that "[...] the need for the transfer is not proven [...]" (Article 29 Data Protection

Working Party 2002: 6). If transfers were to be put on a legal basis, it called for a common European approach (ibid: 8).

The talks picked up speed with a joint declaration by the Commission and CBP, dated 17/18 February 2003 (European Commission / US Customs 2003). In this declaration the EU assured the USA of its "full solidarity" in fighting terrorism, but then focused on the need for "practicable solutions that would provide legal certainty for all concerned" as its prime objective. Already at this time the European Parliament complained about not being kept up to date by the Commission and criticised the joint declaration as having no legal basis (EP 2003b). When the 5 March 2003 deadline for implementation approached, the Commission asked the US for more time, urging member states to do the same (Council of the European Union 2003). The deadline passed without an agreement, and transfers began on an interim basis.

In a debate at the European Parliament on 19 March 2003 (EP 2003a) Commissioner Bolkestein defended this interim solution: "The stakes, therefore, were very high and the consequences of not acting would have been extremely serious". He went on to describe the balancing act needed in the issue – balancing not between privacy and security, but between privacy and jobs in the airline industry. He deemed the unilateral US approach "unacceptable", but pointed out that not talking to the USA would have been even worse. For the future, he called on the USA for earlier consultations to avoid "political difficulties that we have had from time to time over the last year", saying that they did not take European concerns seriously at first. Parliamentarians from all groups expressed dissatisfaction with the Commission's information policy (EP 2003a). Parliament went on to adopt a resolution accusing the commission of failing to check whether the U.S. demands were really covered by American law, failing to inform the public and in general, failing to handle the issue in a timely manner – it had been on the table for 15 months, yet no official initiatives had been suggested to Parliament and the Council (EP 2003b). The issue was primarily addressed in terms of possible privacy violations, with references to economic consequences. The resolution did not contain any references to PNR as a security measure. Parliament also suggested a trusted third party act-

ing as a clearing-house for PNR data, the so-called Austrian Proposal. This idea did not gain traction in the negotiations (EP 2003c).

Commissioner Bolkestein did not question the use of PNR data for security purposes as such; instead he insisted that "[w]e must be realistic" in responding to the demands, pointing out that other states would follow suit on the USA's demands (Bolkestein 2003c: 2). He recognised that the issue was "a conflict of laws, but not just that"; according to him, the Americans had a "different approach when it comes to the security of their homeland" (Bolkestein 2003a). The main task was thus to ensure a uniform solution for all of the EU so as not to disrupt the internal market. In this vein, the Commission staff labelled the issue as a legal problem in which a "solution [was] urgently required" (European Commission 2004b). The reasoning behind this was that if data protection authorities in some member states were to taken action against the transfer while others might not, this would distort the common market. The Commission also called for a "global EU approach", establishing a multilateral framework for the use of PNR under the umbrella of the ICAO (European Commission 2003). Such proposals were put forward in 2004 (European Commission 2004c; Council of the European Union 2004b).

The Article 29 Group kept on criticising the planned path from a legal perspective (Article 29 Data Protection Working Party 2003). While the U.S. slowly offered more concessions over the course of the summer (Bolkestein 2003a), the European side wasn't satisfied yet. Only in early December, a favourable adequacy decision began to seem possible (Bolkestein 2003b). After further concessions, agreement was reached in principle on 16 December 2003 (DHS 2003c), with only some questions remaining, such as the possible use of EU-sourced data for CAPPS II (Bolkestein 2003d). In this round of negotiations, "the security side was a bit neglected" (interview with a commission official, November 2010).

In March 2004, the Council asked Parliament to consider the draft agreement under to the urgency procedure (Council of the European Union 2004c). It denied this request, and the next round of debates in the European Parliament dealt with the consultation procedure for the agreement and the adequacy decision in the end of April 2004.

Before these debates, Parliament had already adopted a resolution setting out its view on the matter (EP 2004h), which largely echoed the Article 29 Group's criticism (see Article 29 Data Protection Working Party 2004a). It called on the Commission to draft a new adequacy decision, criticising that it was only based on administrative commitments by CBP which could be rendered moot by bureaucratic reorganisations. The resolution also included a list of requirements for an acceptable agreement, notably only transferring API data on an automatic basis, while PNR data should be transferred on a case-by-case basis for combating an enumerated list of serious crimes, an independent redress mechanism, an instant block on the "pull" mechanism, and a list of agencies with whom CBP could share transmitted data. It also noted that it would to agree to urgency procedures for an agreement that fulfils these demands (EP 2004h). Commissioner Bolkestein dismissed these demands as "pie in the sky", saying that a deal had absolutely to be reached: "We can only influence the United States if we are credible interlocutors. Credible interlocutors deliver results." (EP 2004g).

In the debates in late April, the council framed the agreement as a necessary compromise. In the words of Dick Roche (Irish presidency, Minister of State for European Affairs): "The deal which has been worked out by the Commission is a necessary one. In the circumstances it is a good deal. The status quo is unsustainable."; a failure to sign would also cause trouble for the airlines (EP 2004c). This sentiment of necessity was echoed by External Relations Commissioner Christopher Patten, who asked rhetorically: "Do we wish to be taken seriously in this realm or not?" (EP 2004c). He also announced starting policy a dialogue on security with the USA in which officials could meet and exchange ideas.[8] Patten also promised a shift to a "push" system "as soon as possible" (EP 2004d). Some issues, such as the rules for onward transfers of transmitted data to third countries, were still under negotiation at that time, as Commissioner Bolkestein admitted, claiming they only came to the agenda recently (EP 2004f).

8 DG JHA Jonathan Faull later described these meetings as fruitful and "[...] accompanied by a whole range now of informal contacts between colleagues on both sides of the Atlantic [...]". According to him, the common task would be "[...] to find the best way to use all that modern technology offers us and the best possible human judgment because that's what it comes down at the end of the day." (quoted in DHS 2004h)

All groups except the conservative PPE-DE opposed the draft agreement. While it was the biggest single group, it did not have a majority in the European Parliament. For it, LIBE chairman Jorge Salvador Hernández Mollar endorsed the draft, saying that "[...] nobody can deny that combating terrorism is an absolute priority today [...]" and that "[...] European society, living in fear of those people who threaten their security and stability, would not understand the absence of cooperation between those countries which are facing up to terrorism" (EP 2004d), or to quote his colleague Hubert Pirker: "The war on terrorism must be our first priority." (ibid). MEP Johanna Boogerd-Quaak (ELDR), the rapporteur for the issue, did not share this view: "I agree with you [Commissioner Patten] that terrorism is appalling, but just to use all that as a licence to ride roughshod over our laws [...] is going too far" (EP 2004d). Additionally, she accused the Commission and the Council of having "deliberately tried to sidetrack Parliament" by not informing it on time and trying to cut short its role with dubious legal manoeuvres. In a similar vein, MEP Elena Paciotti (PSE) complained that the agreement "violates one of the fundamental rights of European citizens", the right to privacy, and called for a lawsuit before the ECJ. In the same session, Parliament also rejected a Spanish proposal to establish a European PNR scheme. Later, a lack of information on whether there was added value in PNR analysis was given as a reason for this (EP 2004e).

Afterwards, the EP adopted the Boogerd-Quaak report on the issue, against the votes of the PPE-DE group (EP 2004i). As called for in the report, EP President Patrick Cox again called on the Council not to sign the agreement and complained about the Commission's lacklustre information policy (Cox 2004). The Council replied that, after considering Parliament's objections, as well as "[...] the need to pursue the fight against terrorism which is a priority of the European Union" and possible financial repercussions for airlines if an agreement were not to be concluded "as soon as possible", it would sign an agreement nonetheless (Council of the European Union 2004a). This explanation was taken verbatim from the initial urgency request. Ignoring Parliament's objections, Council and Commission went on to pursue the matter, and an agreement was signed in Washington on 28 May 2004 (EU-USA PNR Agreement 2004). Looking at the agreement itself, it stressed "[...] the importance of respecting fundamental rights and

freedoms, notably privacy, and the importance of respecting these values, while preventing and combating terrorism and related crime […].” (EU-USA PNR Agreement 2004. This is the only reference to security issues in its recitals, the rest of it sets out the legal background.

As shown, the issue was framed differently on both sides of the Atlantic, and also within Europe. While the majority position of the EP (and the Article 29 Group, obviously) took it to be primarily a data protection matter, the Commission set its focus on market and competition issues, a position partly echoed by the Council, which devoted slightly more attention to security. A common theme for both of them was the desire to be taken seriously, which meant not opposing US demands too much. In Parliament's view, the whole process was intransparent.

The next item to consider is the technical implementation. During the run-up to the agreement, several technical measures to reduce the transfer's privacy impact have been suggested, such as the Austrian proposal (creating an intermediary institution acting as a information clearing-house, see EP 2003c), or double-blind checks (in which the actual data would only be transferred if there was a “hit”, see Baker 2003: 5). Neither of these options was pursued.

After a joint review conducted in September 2005, the European team concluded that in general, DHS was in compliance with its undertakings. However, there were some areas of concern and compliance took longer than expected. The latter point was echoed by the DHS Privacy Office in its own report (DHS 2005a :13). According to DHS's wishes, parts of the review were not made public. The areas of concern were the long time it took CBP to install filters for sensitive data and a lack of complaint mechanisms. Additionally, the switch to a “push” system seemed not to have been pushed forward vigorously (European Commission 2005: 13). The review team also complained about not having had access to all necessary information and being bound by non-disclosure agreements (ibid: 7).

The agreement called for a switch to a “push” system “as soon as this is technically feasible” (EU-USA PNR Agreement 2004) with the CBP undertakings only allowing for “pull” access until this switch was completed (DHS 2004i). DHS claimed to work with

carriers and GDS on switching to such a system (Department of Homeland Security 2005a: 28). The European Team was not satisfied with these efforts and noted that the Commission had been promised that a "push" system would be in place by the end of 2005. Additionally, DHS raised its intention to retain "pull" access for cases in which it decided that data would be needed more 72 hours prior to departure (European Commission 2005:12). Even after the agreement had been annulled by the ECJ in summer 2006 and the interim agreement had been concluded, most carriers were still using the "pull" method (Ntouvas 2007: 94). Out of those airlines that switched to "push", some transferred less than data fields than demanded, for example Austrian Airlines, which only transmitted 10 fields, apparently without repercussions from CBP (Ntouvas 2007: 97).

Implementing the agreed filtering took longer than expected by DHS; the list of sensitive terms to be filtered was finalised on 3 November 2004, long after the agreement has been signed; CBP implemented filtering mechanisms on 14 March 2005. Similarly, it took CBP a long time to be able to tell which data had been accessed manually (which was important, since those could be stored longer). Additionally, CBP only provided mechanisms to deal with requests and complaints relating to European PNR starting 16 May 2005 (European Commission 2005: 10-11)

CBP did not address these issues on its own, it only made changes after being prompted to do so by the DHS privacy office (European Commission 2005: 11). In some areas however, there has been over-compliance: Data access was tracked in a more detailed way than demanded, and sensitive data transmitted under the interim solution had been deleted afterwards, which had not been demanded either (European Commission 2005: 11-12). The DHS privacy office, which oversaw CBP's compliance efforts, noted that support for complying with European demands "[...] must not lose sight of the fundamental and shared security purposes behind the PNR Undertakings [...]" (DHS 2005: 4). The review did not officially deal with the issue of how the data were used and if they led to arrests or were otherwise useful, it was strictly about compliance with the undertakings. During the review, the Commission and the Council

learned of the ATS, but did not make it public until the US administration itself went public about the programme in November 2006 (EP 2006a).

While in general, there has been compliance, two point stand out here: First the fact that CBP had to be pushed to make improvements by the DHS Privacy Office and did not move to implement its obligations on its own. Second the reluctance to switch to a "push" procedure. To recall, the "pull" procedure was the main legal objection on the European side.

To sum up this discussion of the 2004 agreement and its implementation, the matter was discussed differently in the USA and the EU: For the USA, it was mostly a security issue, framed in stark terms as being necessary to fend off terrorists, a clear securitising move. Publicly, evidence for PNR's usefulness was not given, it was just assumed. Whether security professionals lobbied for their use on a working level could not be determined from the documents available. On the European side, different actors set their priorities differently. For the Commission, it was first and foremost a matter of protecting the airlines, with privacy concerns and counter-terrorism coming second. The Council was relatively quiet, with its position close to that of the Commission, accentuating counter-terrorism a bit more. The European Parliament in turn put privacy first, then the airlines, and only rarely mentioned counter-terrorism. It was sidelined by the Council and the Commission (even more so than already by the institutional setup), who only informed it reluctantly. References to the need for privacy were frequent on both sides. However, they should not stop the USA from "doing what is right and responsible" (DHS 2003a), nor preclude the signing of an agreement, lest Europe run the risk of not being taken seriously in the transatlantic relationship (Christopher Patten in EP 2004c).

What happened next? Even before the agreement was officially concluded, the Parliament explored options to challenge it (European Parliament Legal Service 2004), and decided to file two lawsuits before the European Court of Justice shortly after its signing, challenging both the adequacy decision and the agreement itself on formal and material grounds (European Parliament 2004a; 2004b). In the meantime, the EU concluded another PNR agreement with Canada (EU-CA PNR Agreement 2006).

4.2 The 2006 Interim Agreement

The ECJ delivered its judgement on 30 May 2006, invalidating both the agreement and the adequacy decision because the community's first pillar was not the right legal basis (Ntouvas 2007). The court allowed for a transition period until the end of September 2006. A new agreement had to be reached by then. In the meantime, Secretary of Homeland Security Tom Ridge had resigned on 30 November 2004, and the renegotiations were handled by the new secretary Michael Chertoff and his new senior staff. Both Chertoff and his staff were more critical of obligations under international law and less accommodating to European wishes (see for example Chertoff 2006b), a change that was felt in the negotiations: “I saw the change and it wasn't for the best” (interview with a Commission official, November 2010). Or, as seen from the other side by Assistant Secretary for Policy Stewart Baker: “If I'd been here last year, DHS never would have signed that agreement” (Baker 2010: 104). American intelligence services maintained an Al Qaeda threat to aviation (DHS 2004f).

How did the two sides react to the ECJ decision? The USA appreciated the earlier opportunity to the renegotiate the “unacceptable” (Baker 2010: 108) agreement and sought terms more favourable to its interests, notably easing restrictions on transferring data to other agencies. In turn, the EU suggested to first simply switch the old agreement onto a new legal basis in the third pillar – including a sunset clause – and then to negotiate for a completely new agreement to be concluded in 2007, as was planned anyway. This view was also reflected in the negotiation directives (European Commission 2006c). In parallel to these renegotiations, the old agreement had to be denounced (Council of the European Union 2006c).

In the meantime, DHS had also finished an internal review – the so-called “Second Stage Review” – one of whose results was the perceived need for improved information sharing within the Department and with external partners (DHS 2005b). In Secretary Chertoff's words: “The ability to share information with our international, state, and local partners, the private sector, law enforcement and first responders is absolutely critical to our success.” (DHS 2005i). Before, all US security institutions had been obliged to increase their sharing of counter-terrorism intelligence, obliterating what little was left

of the “wall” between intelligence and criminal justice functions (Intelligence Reform and Terrorism Prevention Act 2004). An increased reliance on risk analysis and intelligence was a common theme throughout DHS publications (see e.g. (DHS 2005c; 2005d; 2005e). The need for more international sharing was stressed as well (DHS 2006a). To sum up DHS's attitude: “The principal weapon we have in the war against terror is information.” (DHS 2005e). This emphasis on information collection and sharing was shared by the intelligence services as well (Baker 2010: 112). The last remnants of the “wall” were to be eliminated: “We need to fuse that information and combine it with information from other members of the intelligence community [...].” (DHS 2005i). Additionally, DHS wanted to improve its capabilities for intelligence collection and analysis (DHS 2005g) in order to play a bigger role in the intelligence community, for which improved own capabilities were a necessary prerequisite. “By having more to contribute, first of all, we will have frankly more vigorous place at the table”, in the words of Secretary Chertoff when addressing the Senate Homeland Security Committee (DHS 2005h). Better own intelligence capabilities were also wanted to improve DHS's so far weak standing in the inter-agency process (Baker 2010: 112-118). This focus on intelligence was also justified by the supposedly new nature of the adversary: “So, we must respond by examining the 21st century structures and systems that terrorists exploit in order to carry out their missions so that we pinpoint the vulnerabilities and shut them down. In most networks, vulnerability points tend to be in communication, financing, and transportation” (DHS 2005f).

In justifying its demands for more access and easier sharing, DHS kept on invoking the existential threat posed by terrorism: “We are fighting an enemy who will not rest until its dark vision of the future is achieved.” (Chertoff 2006c): 10). In this fight “[...] we still remain handcuffed in our ability to use all available resources to identify threats and stop terrorists”, wrote Chertoff in an opinion piece for the Washington Post referring specifically to the EU-USA PNR agreement (Chertoff 2006a). “Apart from known terrorist threats, we also need to be able to identify unknown terrorist threats – that is, people who don’t appear on any watch list or in criminal databases” and PNR are “one of our most valuable tools” to do so (Chertoff 2006c), as they “[..] can be analyzed in

conjunction with current intelligence to identify high-risk travelers before they board planes." (Chertoff 2006a). Keeping suspected terrorists off planes was seen as a shared objective among all governments: "All governments bear a responsibility to prevent terrorists from boarding aircraft, and information sharing is a critical way we can work together to limit terrorist mobility, screen for unknown threats and investigate terrorist cells." (ibid). According to Chertoff, this would not lead to a loss of privacy: "Indeed, more data sharing leads to more precisely targeted screening, which actually improves privacy by reducing questioning and searches of innocent travelers" (ibid). DHS also advocated the creation of a "security envelope" for trusted travellers, separating them from those on the outside, on whom analysis and vetting would be concentrated (DHS 2005f). To do this, "[...] we need to get information not only from within this country, but from abroad about people who are traveling." (DHS 2005e). This in turn led to greater demands for information sharing: "[...] sharing ha[s] been critical to dealing with the threat of terrorism globally. We need to continue to advance on that front. Both the U.S. and EU have done a lot within our respective borders to strengthen law enforcement coordination. Now, we must move aggressively to do the same across the Atlantic." (DHS 2005f). The need for international sharing is also emphasised by the fact that terrorism is usually framed as a threat coming from the outside:

> "That means even as we pursue terrorists overseas, we work at home to prevent infiltration by terrorists and their weapons; to protect our people and places if infiltration occurs; and to respond and recover if an attack is carried out. This is embodied in our strategy of building multiple barriers to terrorist attacks." (DHS 2005c), see also (DHS 2005e).

The public statements just claimed that the data were useful. No concrete examples were given in public. Even in the negotiations themselves "[...] unfortunately the examples they give, which even to me are only sometimes in outline, are very highly confidential", complained DG JHA Jonathan Faull, who headed the Commission's team in the negotiations when interviewed by the British House of Lords. "That has been repeated over the months and years during which we have been discussing these issues with the United States", continued Faull (House of Lords 2007, evidence: 40).

Summing up DHS's rationale: Terrorists come from abroad and can be detected via intelligence collection which in turn makes it indispensable for US authorities to have access to as much data as possible. Risks, such as data abuse or taking wrong decisions, aren't considered. Concrete evidence for PNR's usefulness was not given in public, their usefulness was believed to be obvious. Even in the negotiations themselves, evidence was scarce. To cut it short: "The transfer of PNR data by air carriers to our department is an absolute necessity to safeguarding air travel and public security." (DHS 2006c).

This sentiment was echoed on the other side of the Atlantic by Home Affairs Commissioner Franco Frattini: "In order not to endanger public security, all efforts should be made to ensure that this agreement replaces the current one at the time when it expires […]." (European Parliament 2006d). Similarly, the Council Presidency maintained that having a new agreement by 1 October was of "utmost concern" (Council of the European Union 2006b). This time, the negotiations were officially led by the Council, assisted by the Commission. The Commission did most of the work, though. In the inter-agency process, the other commissariats involved (transport and external relations) wanted only minor changes to the draft produced by DG JHA (European Commission 2006a). The negotiation directives adopted in late June called for a simple re-adoption of the agreement on a different legal basis (European Commission 2006c).

Although the European Parliament had no formal powers in the issue – due to the new legal basis – it kept on raising the topic. It urged Commission and Council to use the "passerelle" clause to allow for a bigger role for it in the future (European Parliament 2006d; 2006g). Frattini supported this idea when speaking in the European Parliament (European Parliament 2006d). DG JHA Faull endorsed it too and the incoming Finnish presidency wanted "to open a dialogue" on it (Council of the European Union 2006b). This went nowhere. As British liberal MEP Sarah Ludford said: "[...] I am afraid too many of us are preaching to the converted: it is the Council that we have to convert." (European Parliament 2006b).

In the debates organised by the European Parliament, which constituted most of the few public justifications for the negotiations, MEPs frequently expressed frustration at the Council's information policy – they complained about finding out about new propos-

als from the press, Council representatives leaving the debates early or not showing up at all. This attitude was echoed in all political groups in the EP (see e.g. EP 2006c; 2006d), with Wolfgang Kreissl-Dörfler (PSE, Germany) calling the Council and Commission performances at the LIBE committee meetings "embarrassing", and saying that "[...] the Council is in disgrace" for not being present at the debates (EP 2006d).

In terms of content, Parliament was in favour of a higher level of data protection and cautioned against cutting debates short. French Social Democrat MEP Martine Roure stressed that an interim agreement "[...] must not be hastily negotiated." and urged to implement a "push" system (EP2006d). In the words of Dutch Liberal MEP Sophia in't Veld, there was no opposition to an agreement as such, "[...] there should be data-sharing, because we all want a safer world and to fight the scourge of terrorism, but [...] this should be proportional. We should not share more data than is strictly needed to achieve our purpose." (EP 2006d). Wariness towards American use of the data, as voiced by British Liberal Sarah Ludford, was widespread: "The Chertoff vision is of data-mining and profiling on the basis of past and assumed future behaviour and stereotypes of potential terrorists." (EP 2006d).

Parliament's Civil Liberties Committee also issued a report in which it urged stricter purpose limitations for transferred data, an evaluation of which data fields were really needed, shorter retention periods, an immediate switch to a "push" system, as well as better means of legal redress in the event of abuse (Committee On Civil Liberties Justice And Home Affairs 2006). It also expressed fears that any EU-US agreement would become the standard against which future proposals, e.g. in the ICAO would be measured, and so would institutionalise lacklustre privacy protections (ibid: 10).

After these debates, the European Parliament adopted a resolution (EP 2006e) based on the LIBE Committee's report. In it, Parliament said it was in favour of an interim agreement to avoid a legal lacuna, but urged for it and any new agreements to be based on the respect for private life as laid out in article 8 of the European Convention of Human Rights (EP 2006e: 4). While Parliament appreciated the "expressed willingness" of the Commission and the Council to cooperate, it also said it was "[...] regretting that the Council has failed to involve the Parliament in the ongoing negotiations" (EP 2006e: 3).

For the longer term, a framework for the use of PNR should be developed under the umbrella of the ICAO. The text contains no direct references to the usefulness of PNR for security purposes, instead it expresses fears that with the immense number of security measures enacted since 9/11, "[...] the position of the individual citizen vis à vis the state risks being undermined" (EP 2006e: 2).

After both sides had finalised their negotiation mandates, the first meeting happened on 8 September 2006 (EP 2006f). After the US made it clear that they were not afraid of letting the agreement expire and unilaterally demand data transfers without any of the safeguards provided in the Undertakings, the European side found itself in retreat (Baker 2010: 126).

During the negotiations Frattini was perceived by the American side as a faithful representative of the Commission's positions, "[...] but when push came to shove, he was on the side of law enforcement", with his "practical experience" (as former Italian Interior Minister) enabling him to "[...] reach across the Atlantic and find common cause with Chertoff whenever tensions arose" (Baker 2010: 134). DG JHA Faull similarly expressed understanding for American security concerns, saying "[...] the rational basis on which a decision will have to be made on this will be finding out all we can about the genuine needs of law enforcement and counter-terrorism investigators based on their past experience [...]" (House of Lords 2007, evidence:45). When the deadline expired and airlines continued supplying the data, no flights were cancelled and no enforcement action by data protection authorities were started, European demands for better data protection standards found even less traction (Baker 2010: 136).

After the agreement was initialled in early October, the Presidency and the Commission went to defend it in the European Parliament (EP 2006c). The presidency, represented by Finnish Minister for Foreign Trade and Development Paula Lehtomäki, said the agreement was a success because of the security gain it provided:

> "The outcome of the talks is a success for many reasons. Firstly, the temporary arrangement aims at ensuring the security of air passengers. This is vitally important. Secondly, I wish to stress that the commitments on the use of PNR data given previously by the US administration will continue to apply." (EP 2006c)

The latter part was not completely true, as the DHS side letter significantly altered these commitments and allowed more sharing (see Council of the European Union 2006a for its text and the section on technical implementation below for a discussion). Commissioner Frattini shared Lehtomäki's assessment and also announced increased EU-US-cooperation for the future:

> "This agreement forms part of a wider commitment. I can of course say that, during the very complex negotiations that have been in progress, both the European institutions - the Presidency and the Commission - and the United States have confirmed their willingness to start straight away on a shared project. This would cover a wider field and would thus include the reaffirmation of a common will [...] to work towards a definite agreement [...] and to cover the widest possible field of joint cooperation against terrorism, together with protection of the rights of the individual."
> (EP 2006c)

Compared to how the Commission defended the first agreement in the Parliament, the change is obvious. Frattini downplayed the repeated concerns voiced by Parliament, because "[o]therwise, we risk forgetting that the problem is terrorism, not the US." (European Parliament 2006c).

After adopting a Council decision on the agreement (Council of the European Union 2006e), it was signed on 16 October 2006 (Council of the European Union 2006d). In the agreement itself, the reasons given shifted compared to the first one. Now, the desire to "prevent and combat terrorism and transnational crime effectively" came first, before noting that a legal arrangement should govern the transfer of PNR, and only then recognising that privacy should also be protected while fighting terrorism (EU-USA PNR Agreement 2006).

Even though the content of the agreement itself wasn't changed much, DHS gained additional rights to use the data by issuing an interpretation letter. Before addressing this issue, let us look back at this round of negotiations. For the Council and the Commission security concerns came first, privacy considerations second, worries about the airline industry were a lot less prominent. The agreement was supposed to be "vitally important" for the security of air passengers, and necessary "not to endanger public security" as "part of a wider commitment" to improve transatlantic cooperation. Again, ac-

cording to them, there was no viable alternative to the deal that had been struck, even though no evidence had been supplied to the public. Parliament's calls for proportionality went unheard.

Turning to the implementation of the agreement, DHS's side letter altered the terms drastically, while the switch to "push" did not proceed. Under the agreement, DHS was entitled to issue unilateral letters advising the EU of changes in domestic legislation that affected the data's use, a possibility Faull hinted at first (Baker 2010: 126). This letter (Council of the European Union 2006a, annex 3) reinterpreted the agreement, stretching the term: "Of course, it went well beyond what most lawyers would call interpretation." (Baker 2010: 129). Referring to the Intelligence Reform and Terrorism Prevention Act of 2004, DHS informed the EU that it would share date with less restrictions in the future. This act did not contain provisions specific to PNR, it only demanded that security agencies share intelligence on terrorism in a "Federal Information Sharing Environment" – demands that, read broadly, could be used to ease the restrictions on onward transfer, since according to the 2004 agreement, DHS was entitled to change its implementation if compelled to do so by domestic law (Baker 2010: 126-127, 129-130). In the letter DHS stated that "[...] the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating of terrorism and related crimes [...]" (reproduced in Council of the European Union 2006a: 12). This altered the possible uses radically, erasing many of the restrictions originally imposed by the agreement.

The agreement called for a switch to a "push" transfer as soon as technically feasible, and this time included a deadline on 1 January 2008 for carriers technically capable of it. Frattini claimed in October 2006 that the EU had written assurances from the US that this switch would occur "by December at the latest" and that "the 'push' system can come into operation from tomorrow." (EP 2006c). The Finnish Council Presidency said the same (Council of the European Union 2006f). After this date passed, DG JHA Faull said next spring that DHS would be "happy" to switch to "push" (House of Lords 2007, evidence: 44). The technical preconditions appear to have been in place since summer 2006 at the latest (Council of the European Union 2006b). Data protection authorities

similarly said that a switch to "push" could happen any time soon because "[…] the air carriers have implemented the necessary technical infrastructure and there are no plausible reasons for any further delay." (Article 29 Data Protection Working Party 2006 :3). However, for most carriers, DHS still used the "pull" method. It also claimed the right to "pull" under certain circumstances, even if the carrier in question had already switched to "push" (Hobbing 2008:47). According to the British Information Commissioner, airlines and DHS blamed each other for failing to switch to "push" (House of Lords 2007, evidence: 57). The EC-Canada PNR-Agreement, which had been concluded in the meantime used a "push" system, apparently without problems (EP 2006c). No complete switch to "push" occurred during the time the agreement was valid, only three carriers had implemented "push" by summer 2007 (European Commission 2010): 25). The Commission also promised to raise the topic of the use of European PNR for ATS with the USA, of which it apparently learned during the 2005 joint review (EP 2006a). Since the participants were bound by non-disclosure agreements (see European Commisson 2005: 7), this information did not reach the public nor parliamentarians. In fact, the USA only publicly acknowledged the existence of this program in November 2006 (American Civil Liberties Union 2007).

To sum up the interim agreement's justification, DHS still framed the transfer as indispensable for providing security. New elements were added in the notion of a "security envelope", references to protecting privacy or balancing it against security needs became fewer; in fact, increased data transfers were claimed to enhance it. On the European side, the issue was more framed as a security issue, rather than as a trade issue, as it had been the case in the first round of negotiations. While the security use of PNR was barely mentioned by the European side in the first round of talks, it became prominent in this one. As the European Parliament had no official role to play, its concerns were ignored. Even if the text of the agreement itself was barely changed, DHS's interpretation letter opened up new possibilities for sharing the data. On the technical side of things, a switch to a "push" system was promised again, but not fulfilled, with apparently a lot of inertia on DHS's part.

4.3 The 2007 Agreement

Negotiations for the follow-up agreement started shorlty after interim agreement's signing and were again conducted in the third pillar, this time under the Finnish and German presidencies assisted by the commission. They were finished faster than expected (Papakonstantinou and de Hert 2009: 907), in the words of the American chief negotiator “almost anticlimactic” and with “far less drama” (Baker 2010: 140-141).

On the US side, access to PNR was still framed as an indispensable means of security: “If we surrender this tool, we will abandon the real-time defenses that can save our citizens' lives.” (Chertoff 2007). A new development was that now examples were used more often, including the claim that 9/11 could have been prevented, had law enforcement agencies already had access to PNR. Secretary Chertoff stressed PNR's utility when addressing the European Parliament: “We are collecting it because time and again it is proving to us that it will enable us to keep dangerous people outside the United States” (DHS 2007a). Preventing undesired persons from entering the US was also emphasised in statements aimed at domestic audiences, for example when he addressed the House of Representatives' Homeland Security Committee: “Our aim is to intercept dangerous enemies abroad, before they reach our borders.” (DHS 2007f), claiming that using PNR, API and ATS “[...] we have identified overseas passengers who have posed a real danger and prevented them from entering our country.” (DHS 2007f). Similarly, before the Senate's Homeland Security Committee, he said: “If we can prevent dangerous people from infiltrating our borders then we have successfully dismantled a large part of the threat” (DHS 2007g). PNR were said to “have helped us significantly in combating potential threats” (DHS 2007f) and “[...] continued access will be invaluable in the fight against terrorism and successfully protecting our borders by keeping dangerous people from boarding planes and entering the U.S.” (DHS 2007b).

Again, the need for information sharing was emphasised: “One of the central lessons of the 9/11 attacks, and subsequent attacks in Europe and elsewhere, is that we must break down barriers to information sharing.” (Chertoff 2007). This attitude was shared throughout the US administration, for example by Attorney General Alberto Gonzales, saying that “[...] one of the things we're working through is trying to get as much in-

formation as we can that's absolutely necessary to help us identify potential threats." (DHS 2006c). If it stuck too strictly to adequacy requirements, Europe was running a "[...] very real risk of turning itself into a self-imposed, isolated island from the very allies it needs", claimed Paul Rosenzweig (DHS Deputy Assistant Secretary for Policy), who went on to criticise the proposed framework decision for a European PNR system as seeking "to apply the same tired, failed standards of adequacy" the EU applied to commercial issues (quoted in Hobbing 2008: 50).

A variety of different examples were used on several occasions (e.g. (DHS 2007f) (DHS 2007g), with the longest list outlining eight cases – which included all the examples used in the other documents – being part of a letter with which Chertoff tried to convince MEPs of the necessity of PNR transfers. Half of these referred to drug trafficking cases, with the other half referring to persons denied entry or boarding due to being "linked" to terrorist suspects (Chertoff 2007).

When Chertoff addressed the European Parliament in person in May 2007, he kept up the strong rhetoric: "I believe we are at war [...]" (DHS 2007a). According to him, a new approach was needed to fight Al-Qaeda, claiming that it was a new threat unlike previous terrorist problems, based on statements by the head of Scotland Yard's counter-terrorism unit. Intelligence was paramount here; terrorists "[...] can only be detected by the use, analysis and sharing of intelligence that allows us to separate those who are a threat from those who are innocent." (DHS 2007a). This in turn would also spare non-suspicious travellers inconveniences. PNR were important for finding connections between known suspects and other travellers: "It is the ability to use this information to identify hidden connections that makes it so valuable as a tool to keep out dangerous people." (DHS 2007a).

Again and again, DHS stressed that "Passenger Name Record data is a proven tool for combating terrorism and serious transnational crime, providing the U.S. with the means to make connections between known threats and associates and identify patterns of concerning activity." (DHS 2007b). This notion of PNR being necessary for "connecting the dots" shows up in several DHS documents (DHS 2007c; DHS 2007i).

To alleviate privacy concerns, DHS pointed out that the agreement demanded the treatment of European PNR with the same standards that apply in domestic American legislation (Chertoff 2007; DHS 2007a). Chertoff made the claim that PNR transfers could actually increase privacy: “I believe a clear and compelling case can be made that sharing PNR and other identity information will be a net gain for privacy and civil liberties” (DHS 2007a), as those who are not targeted for secondary questioning can travel with less cumbersome controls: “The key here in a nutshell is a membrane that allows the innocent and the freedom-loving to travel without hindrance, but forces those who would do us harm to stumble as they come in to carry out their attacks.” (DHS 2007h). This echoes the notion of the “security envelope” in earlier publications and once more shows how the threat is seen as coming from abroad.

The short version of DHS's justification can be summed up like this: “We must not take this valuable counterterrorism tool away from border law enforcement professionals by limiting or restricting the kind of information sharing and analysis that has already proven effective.” (Chertoff 2007). DHS saw PNR as a tool that has proven its value and should not be taken away from the professionals. The focus on intelligence collection and analysis is strong in all statements. The lists of examples provided are a change compared to the prior rounds.

For the EU side, the negotiation mandate called for a switch to a “push” system and explicitly mentioned reciprocity (European Commission 2006b). Reciprocity meant that in case a European PNR analysis system were to be set up, American airlines would have to supply PNR as well.

When presenting the Commission's agenda for 2007, Frattini referred to the coming negotiations, in which the Commission “[...] will ensure that security issues are properly addressed through the transfer and appropriate use of PNR data, while protecting personal data as guaranteed by Article 8 of the Charter.” (referring to the European Charter of Fundamental Rights which in article 8 protects private life; EP 2006a). A new agreement would form part of larger anti-terrrorism efforts, since “[o]nly a very solid strategy and balanced cooperation with our main international, transatlantic partner will make it possible to reduce if not eliminate this modern form of totalitarianism against demo-

cracy." (EP 2006a). Earlier, in a joint press conference with US officials celebrating the initiation of a high-level contact group for exchanges between senior officials from both sides of the Atlantic, Frattini had already labelled terrorism "the first threat against our democracies", an assessment shared by the equally present German Interior Minister Wolfgang Schäuble (representing the incoming German Council Presidency) (DHS 2006c). At the same occasion, Frattini also adopted Chertoff's view on the privacy implications of new security measures, saying that "[...] we need [...] to explain [...] to our public opinion that there is no contradiction between more security and more protection of fundamental rights, including privacy protection." (DHS 2006c). The focus should be to "[...] identify [...] commonalities, not focus on divisions and different approaches.", according to Frattini (DHS 2006c). At the same meeting, Finnish Justice Minister Leena Lutahnen stressed the "good cooperation" across the Atlantic, taking PNR transfers as an example, and that the "security interests" of both sides were "in agreement" (DHS 2006c).

When the negotiations started, the German Presidency (represented by Foreign Office State Minister Günter Gloser) said that it was "[...] likely that the negotiations [...] will prove to be extremely difficult, since there is no evidence of any interest on the part of the United States in improving data protection" (EP 2007c), an assessment whose second half bore out more than the first. Frattini framed the proposal's privacy implications quite differently than he did at the joint press conference with DHS:

> "The Commission is recommending to the Council to strive for full respect of fundamental rights, notably the right to privacy. I have said on a number of occasions that the right to privacy is for me non-negotiable. It has to be respected, fully and completely." (EP 2007c)

The difference between this statement and what he said earlier on the occasion of the HLCG's founding is stark. In non-public settings, the sound was harsher, as MEP Sophia in't Veld, Parliament's rapporteur for the agreement said when testifying before the House of Lords about the plans for a framework decision for the use of PNR in Europe: "If you then look at what they say to each other when they believe nobody is watching it is very frightening [...]" (House of Lords 2008), evidence: 35). She also complained about the talk of "balancing" being empty in the absence of evidence: "Mr

Frattini says, 'I believe that it is necessary'. If the Government proposes to spend 20 million on infrastructure works, would you say, 'I accept it as a Member of Parliament' if they say, 'We believe it is useful'?" (House of Lords 2008, evidence: 33). Or, as she demanded on a different occasion when Frattini defended the plan in Parliament: "We need evidence and not just anecdotes" (EP 2007d) and Chertoff's "horror stories" (House of Lords 2008, evidence 32-33) with purported successes in the negotiations such as the claimed reduction in data items to be transmitted being "insult to our intelligence" (EP 2007d). While the negotiations went on, the security function became more important in the public justifications, being mentioned first, before addressing data protection and economic consequences. Again, the agreement was seen as being without alternative, as asked rhetorically by Franco Frattini when addressing the Parliament: "Can any of you imagine that the airlines would have negotiated bilaterally with the United States and achieved a better level of personal data protection? I do not think anyone can even imagine that that might have happened." (EP 2007d).

In the negotiations, the Commission wanted to take a somewhat tougher line on privacy than the German Council presidency; the Council urged the commission to concede, which it finally did (interview with a commission official, November 2010). Within the Commission, Frattini pushed the idea of a European PNR system and was the biggest advocate of the EU-US agreements (House of Lords 2008, evidence 31). He was also in favour of the establishment of PNR systems at the national level "in as many Member States as possible" (EP 2007d). In the Council, France and the UK were the biggest promoters of the idea besides the German Presidency (House of Lords 2008, evidence 32). The UK had already enacted a national PNR collection system which was mostly meant to enforce immigration law (House of Lords 2008, evidence: 5). France and Denmark had also enacted similar laws (European Commission 2007b :3).

Both during the run-up and the actual negotiations, Parliament complained about a lack of information (see EP 2006a; 2006b; 2007a; 2007c; 2007d; 2007e). On a working level, there were informal contacts with the Commission, while Sophia in't Veld, Parliament's rapporteur for the issue summed up (especially the Finnish) Presidency's information policy as "[t]hey have done nothing." (House of Lords 2008, evidence: 33), and

resorted to unusual information channels, since “fortunately minutes of secret meetings tend to fall off the photocopier” (ibid, evidence: 28). This was also mentioned in the resolution Parliament passed shortly before the agreement was signed. It criticised the assurances made by DHS as not binding enough, the “largely cosmetic” reduction in data fields, the extension of retention periods and the EU's commitment not to interfere with forwarding the data to third states. It also called on Commissioner Frattini to clarify his ideas for a European PNR system (European Parliament 2007f).

The Agreement itself repeated the first recital from the 2006 agreement on the importance of fighting terrorism and transnational crime to protect “democratic societies and common values”, before explicitly pointing out that that “[...] information sharing is an essential component in the fight against terrorism and transnational crime and that in this context the use of PNR data is an important tool”, and only later noting that privacy should be protected as well (EU-USA PNR Agreement 2007).

After the agreement had been signed in July 2007, Frattini further pushed the idea of a European PNR scheme:

> “Up until now, PNR has been associated mostly with negotiation aimed at ensuring that European citizen data are processed correctly by our partners and allies, in particular the United States. I think the time has come to partially change focus and devote resources to the security of the European Union. The Union is at least as much a potential target of a terrorist attack as the United States and the use and analysis of PNR is an important law enforcement tool to protect our citizens, who deserve the same protection as the citizens of the United States.” (EP 2007b)

Compared to how Internal Market Commissioner Bolkestein framed the issue in the first round of negotiations, two changes are striking: First, the usefulness of analysing PNR is accepted without doubt instead of being an afterthought to the main question of how to ensure legal certainty from a market point of view. Second, the topic of an own PNR scheme is raised. While security concerns already became more prominent in the second round, the idea of an own PNR scheme had not been pushed so aggressively before. Later that year, the Commission tabled proposals for a Framework Decision (European Commission 2007a;see also European Commission 2007c).

After this small detour to plans for a European PNR system, let us return to the technical implementation of the EU-US agreement. As a joint review has been conducted in early 2010, there is more information on its technical implementation available (DHS 2010a; European Commission 2010b). The new longer retention period of 15 years is split into seven years in an "active" and eight years in a "dormant" database; for accessing data in the latter, a senior official's approval would be needed. This distinction was basically meant to "cushion the public reaction" and would not impede the utmost exploitation of PNR data (Baker 2010: 141). For the technical details see DHS's privacy report on the agreement (DHS 2008a: 35-36).

The agreement also demanded an immediate switch to a "push" system for airlines that have the necessary technical prerequisites in place, a development touted by DHS: "Air carriers will now transmit PNR data directly to the department." (DHS 2007c). Only two European airlines had already switched to "push" by Summer 2007 (European Commission 2010): 25). At the time, the IATA expected a transition period of six months maximum for the other carriers (quoted in EP 2007d). In a document submitted to the ICAO, the IATA later complained about unreasonable demands in implementing "push" (ICAO 2008: 3-4; although the USA is not identified as the state in question, this can be deduced when read in conjunction with European Commission 2010b: 25). DHS claimed to have done what it could to help airlines switch, noting on multiple occasions that it could not legally force airlines to adopt the new system (DHS 2008a: 31-32; 2010a; 2010c). The Commission's report on the joint review conducted in February 2010 notes that "push" still has not been completely adopted and urges DHS to work better with carriers to help them make the switch (European Commission 2010b: 5-6). According to the newest data available (March 2010), 15 European carriers now use "push". For comparison, 43 carriers world-wide use this system (European Commission 2010: 25). Even after a switch to "push", DHS reserves the right to "pull" in certain circumstances when PNR do not have a US nexus. This includes diverted flights and emergency landings as well as refuelling stops and information on passengers who have been refused boarding (DHS 2010c: 6; European Commission 2010b: 18-20). Not all members of the review team could take part in all parts of the review – for example, only the

one external law-enforcement expert was allowed to watch the databases being operated in real time (European Commission 2010b: 8-9)

This review – in contrast to the 2005 evaluation – also contained information on how the data was actually used. The European review team was convinced that the use of PNR by DHS actually enhances security, stating that is "[...]follows a logical approach and maximises the added value of using such data for law enforcement purposes." (European Commission 2010b: 17). On the one hand, PNR are used to check passengers against a wide range of law enforcement databases; this would theoretically be possible with API data as well. Since PNR are usually available 72 hours prior to departure, while API data is only transferred 15-60 minutes prior to launch this gives DHS more time to carry out the checks, which are then repeated with the actual API data in case there is a match (DHS 2007d; recall that PNR are less reliable than API, see European Commission 2010b:15-17). However, they are not run against the Terrorist Identities Datamart Environment (TIDE), the central classified terrorist watch list. The European side criticised that some of these databases – such as one on refused visa applications – were mainly related to immigration issues, and thus outside the agreement's purpose limitation (European Commission 2010b: 17). DHS's reply to this charge pointed out differing interpretations of what constitutes a "transnational crime" as a reason for this mismatch (DHS 2010a: 5; there is no definite list). On the other hand, PNR are also checked against a set of "scenario-based rules" (European Commission 2010b: 15). These rules help DHS to discover previously unknown persons who might pose a risk. They are generated by analysts at the National Targeting Center–Passenger. The rules focus on travel patterns, are changed or amended frequently, sometimes on a daily basis. If a person raises suspicion under these rules, additional manual checks to find associates are carried out. Targeted persons are marked for special attention by boarder guards. The decision to clear the person, deny entry, to refer to secondary screening or to arrest is made by the officer at the border (ibid: 15-17). Some of these rules are developed together with the Canada Border Service Agency; hits under these common rules are forwarded to Canada. DHS does not consider this a "bulk exchange" (European Commission 2010b: 29).

Information derived from PNR may be shared with other authorities on a case-by-case basis (on DHS's approach to data sharing in general see also the DHS Information Sharing Strategy: DHS 2008b). What constitutes a case is interpreted widely; it can be anything DHS is investigating (Baker 2010: 141-142). In 216 cases DHS shared data with other US authorities, mostly with the Department of Justice and its subordinate agencies (including the FBI). According to DHS, three quarters of these exchanges were related to terrorism (European Commission 2010b: 29). Only in one case have PNR been used in criminal proceedings (European Commission 2010b: 14). DHS did not transfer information back to Europol or Eurojust, a possibility that was provided for in the agreement. In one case, information has been transferred to a EU Member State, at that state's request. Under its commitments, DHS should have promoted this exchange more proactively (European Commission 2010b: 35). When this was pointed out, DHS said it was in favour of more sharing as well (DHS 2010a: 5). Both sides had already pledged better cooperation in the Toledo Declaration which was signed shortly before the review meetings (EU-US Joint Declaration on Aviation Security 2010).

In conclusion, what changed in this round of the negotiations? On the European side, security purposes achieved more prominence in justifying the agreement and plans for a European PNR collection scheme gained traction. For the American side, justifications remained largely unchanged. PNR transfer was still seen as an essential measure to ensure security; the main difference was that this time evidence was also offered to the public. This evidence was anecdotal, with a majority of the examples unrelated to terrorism, there were no statistics. How exactly PNR contributed to these successes was rarely elaborated. The rhetoric used by DHS, the Commission and the Council stressed that using PNR was an effective means and indispensable. Again, no public interventions by lower-level security professionals could be seen. The 2010 joint review provided useful information on how the powers conferred under the agreement were actually used, showing how restrictions have been eased. The differing understandings of what constitutes “transnational crime” or “bulk sharing” are examples – the development of common rules with Canada and the mass forwarding of results stretch the terms of the agreement. Implementation of a “push” system is beginning, with 15 carriers now

using it. Compared to the 3 carriers using it at the time of signature. Still, this switch already had been promised in the 2004 agreement, and according to the industry and DPAs, it would have been possible since summer 2007 at the latest. It has to be noted that all of this occurred under provisional application, since the agreement so far has not been officially concluded.

5 Summary & Conclusion

This thesis has set out to take a close look at the issue of PNR data transfer from the EU to the USA. As most prior works on this issue have either focused on the content of the agreements or legal and normative implications, there was a lack of theoretically informed studies of how the agreements came about. In order to address this gap, I proposed an approach drawing on the Copenhagen and Paris Schools.

Arguing that the Copenhagen School lacks social embedding, which can be provided by using insights from the Paris School, I outlined a framework for analysing the relationship between the professionals of politics and the professionals of security. While this approach would have called for a more sophisticated methodology combining discourse analysis and in-depth interviews, this was not possible within the time and space constraints given. This is why a discourse-analytic approach was chosen as a second-best option. Together with the problem that there were few public statements from persons on a working level, this affected how well the framework could be put into practice. The results could have been improved with better access to practitioners in order to conduct more interviews to have a look “behind the scenes”.

Nevertheless, some useful knowledge could be gained. There has been a marked shift in how the issue was presented on the European side. Starting from seeing the main point of the negotiations as to ensure a firm legal framework for airlines to conduct business and to protect the privacy of travellers, security concerns gained more and more traction. From the first agreement to the interim agreement, the policy lead changed from DG Internal Market to DG JHA/JLS, where a security mindset was more widespread, with both staff and the Commissioner expressing more understanding for American demands, which was reflected in the outcome of the talks and their justifica-

tions. Ensuring Europeans' privacy and providing security were now mentioned on equal footing as the main targets for the negotiations, with frequent invocations of the "balancing" metaphor. For the third agreement, the practical negotiations were again headed by DG JHA/JLS. Here, security came firmly first, privacy considerations were set aside, with Commissioner Frattini stressing again and again that PNR were useful and promoting an own European system. In later Commission statements, the usefulness of PNR was taken for granted. The Finnish Council Presidency of the second half of 2006 on the other hand stayed relatively quiet in the public appearances, with Council representatives sometimes not being firm on the issue when addressing the Parliament (see e.g. EP 2006a). Behind the scenes, the German presidency seems to have pushed the issue forward in the first half of 2007. Parliament, on the other hand, stuck to the original framing, putting privacy considerations first and relegating security concerns to a distant second. While there was no room in the empirical parts to elaborate on this, this cannot be purely chalked up to party preferences. It is true that those MEPs who were most vocal on the issue tended to be liberals, greens or social democrats, but conservatives frequently voiced concerns as well. For example, several European Parliament resolutions criticising the agreements were carried by conservatives as well. Summing up, Commission and Council adopted the security framing over time, while Parliament stuck to its initial framing. Its complaints were not addressed by the other institutions, who kept on pointing out that the PNR was "necessary", that there was no alternative. It was normalised as a common-sense tool of law-enforcement.

On the US side, there has been a clear shift between the first agreement and the two subsequent ones. While it agreed to comparatively strict rules in terms of sharing transferred data in the first agreement, the subsequent agreements loosened them. Similarly it pushed for an extension of retention periods, and promised improvements such as the shift to a "push" system were only implemented slowly. In terms of the "push" system, DHS blamed the airlines for not obeying its requirements for the implementation. These were a lot more demanding than those made by other countries that operate PNR systems (ICAO 2008: 3-4). Concerns voiced about privacy were largely met with incomprehension. To address them, DHS either used the common "balancing" metaphor, with

the outcome determined in advance, or claimed that the analysis of PNR actually improved privacy by allowing for a better targeting of controls. During the 2007 negotiations, some examples were provided; the majority of these did not relate to terrorism – the threat that had been used to justify all of the agreements– but drug smuggling and other forms of crime. Nonetheless, PNR analysis was again and again referred to as a "proven tool" that was "indispensable" for defeating the "new totalitarian threat".

Chertoff and Frattini both tailored their arguments to the respective audiences. Frattini was more careful to stress the "balancing" of privacy and security when addressing the European Parliament, pointing out legal obligations imposed on the US. When talking in the USA, he focused more on security gains and the trust between the professionals on both sides (recall his appearance at the joint press conference: DHS 2006c). For the US side in turn, Chertoff was keen to stress privacy protection and successes of PNR analysis when in Europe. When addressing domestic audiences, he stressed the differences instead: "They frankly are much more focused on data protection than we are" (DHS 2006b; Chertoff 2006b).

In terms of technology, it is remarkable how long the still incomplete switch to "push" has taken, even though the technical prerequisites seem to have been in place for years. From the 2010 joint review, it seems obvious that DHS is not committed to finishing this transition. Airlines have complained about overly challenging requirements from DHS, further suggesting that it would like to keep the "pull" system as this gives more control to DHS.

After this summary of the empirical findings, it is time to see how well the theoretical framework performed. Did it yield new insights, could it be appropriately applied?

Instances of lower-level security professionals actively championing security measures could not be observed. This may be because these moves occur within organisations and are not easily visible from the outside. Some of the caveats mentioned in the methodology section apply here. For most of the empirical part, I had to rely on the public justifications. As noted before, gaining access to people at the working level is hard and the public justifications are usually given by high-level officials. This caused problems, as what is said at this level and what is done at the operational level may be

two different things. As for what was actually done, the two reviews provided valuable insight into how the commitments under the agreements and the undertakings were implemented. Nevertheless, the document available did not allow for an analysis on a working level. This hindered going "beyond Copenhagen", because information on what went on behind the scenes was difficult to obtain. So while the influence of security professionals could not be observed directly, it is obvious how much security logic permeated the later public statements. Admittedly, this is not the best proxy. Expanding on this study with interviews to gain a better insight into professional discourses would be an obvious next step.

This takes us to the question on where to go next. Aside from improving on the research done here with more interviews, the framework could be used on other cases. An appropriate target could be the debate on telecommunications data retention; at least in Germany, police authorities are very vocal on this issue, providing for ample material to study. Other candidates include topics such as visa regimes (Salter 2006) and the increasing use of biometrics (Amoore 2006), which so far have usually been surveyed from a bird's eye perspective. Theoretical enhancements could be made in a dialogue with surveillance studies (Lyon 2001; Lyon 2007), or connecting it to organization theory, especially works on institutional autonomy (e.g. Abrutyn 2009). In a different way, the approach presented here can also add to understanding how states react to transboundary security problems (Eriksson and Rhinard 2009): contacts and shared views between the professionals of security in different states are instrumental in bringing cooperation forward. This could also be used to add a comparative dimension to studies of organisational discourses (Martin and Simon 2008).

Turning back to the question of PNR transfer and analysis, how have they evolved outside of the precise topic covered here? The shift towards a security framing and a normalisation of PNR analysis identified above is also echoed elsewhere.

Apart from the agreements covered here, more agreements have been signed with Australia and Canada. Japan, New Zealand, and South Korea use PNR or are testing their use too, but not have not yet entered negotiations with the EU. Saudi Arabia, Singapore and South Africa have enacted legislation on PNR as well (European Com-

mission 2010a: 4). Similarly, plans for a European PNR framework were were put forward. After preparatory work by the Commission (European Commission 2007b), the Council endorsed the idea (EU Observer 2008). At that time, a proposal for a framework decision had been presented, but not adopted. Many governments of member states, especially the UK, advocated for very lax purpose limitations, with the UK going so far as to call for PNR use for all serious crime, organized or not, as well as for immigration matters (House of Lords 2008: 17-18). While several EU member states have enacted legislation for PNR analysis on a national level, the UK is taking the lead, with Meg Hillier, at the time Parliamentary Under-Secretary of State at the UK Home Office claiming that the UK was "ahead of the game." (House of Lords 2008, evidence 12), as the other states did not put analysis systems into place.

The most current developments in the issue include the new EU strategy for PNR transfers to third countries, and the adoption of negotiation mandates for talks on new agreements with Australia, Canada, and the USA.

The strategy, which was published in September 2010 and cannot be analysed in detail here accepts PNR use as an everyday measure of law-enforcement work (European Commission 2010a). This is a marked shift from the earliest communication on this, in which ensuring privacy came first and security concerns were listed under "other policy objectives" (European Commission 2003: 5). The strategy also suggests reintroducing the proposal for a European PNR system, this time as a directive, due to the changes in competences after the Lisbon treaty. DPAs reluctantly welcomed the strategy as "a step in the right direction" because it may help to ensure greater coherence between agreements with different third states. However, they also voiced some concerns, and once more called for evidence of PNR's usefulness, which is simply assumed in the strategy. While law-enforcement authorities may be used to having PNR at their disposal, "[...] that fact alone does not prove political or public acceptance of the collection and use of PNR data, nor does it justify its necessity." (Article 29 Data Protection Working Party 2010). The Commission, on the other hand, maintains that PNR processing "is increasingly seen as a mainstream and necessary aspect of law enforcement work" (European Commission 2010a: 3-4).

In the beginning of December 2010, the Council also adopted negotiation mandates for new agreements with the Australia, Canada, and the USA (Council of the European Union 2010). Although the mandates themselves are classified, they are presumably based on the criteria set out in the Commission's strategy. For the longer term, the Commission is considering looking at options for a multilateral treaty on PNR transfer and analysis, as the current ICAO guidelines on it are non-binding and lack privacy protections (European Commission 2010a: 10). As the matter now falls under the co-decision procedure, the EP will have a say in the issue as well. Whether it will acquiesce to the new agreements to be negotiated is open, given that it still withholds consent to the 2007 agreement. As ratification by national parliaments was slow (Council of the European Union 2009), the agreement had not been concluded by the time the Lisbon treaty came into force and thus now falls under the new procedures. Because it contains a clause on provisional application pending ratification, this did not impede the data transfers.

What still remains to be seen is how this increased use of mass screening will sit with the courts; both the German Constitutional Court and the European Court of Human Rights (Bundesverfassungsgericht 2010; European Court of Human Rights 2008) have been highly critical of blanket data collection in the past. Now that the Lisbon Treaty is in force, the European Court of Justice could again have its say on the issue – recall that the 2006 judgement only addressed formal issues and that its competences include material questions of justice and home affairs as well now.

Whether the “balancing” metaphor can help to find a solution to the discussion is doubtful, for it assumes that liberty and security are communicating vessels, more of one meaning less of the other. This on its own tells us nothing about where an appropriate balance would be (Guild, Carrera, and Balzacq 2008: 8-11; Huysmans 2006: 87-89). Even if one were to accept this metaphor, the absence of reliable evidence makes it hard to arrive at a reasoned trade-off. One possibility would be to give travellers monetary compensation for the use of their PNR – putting a price on them to see if they are really essential to law-enforcement authorities' activities (González Fuster and de Hert 2007). Another difficulty with “balancing” is the question of who balances whose interests –

the privacy of foreigners tends to be valued less than that of citizens; our citizens are their foreigners (Guild 2009: 128-130). For example, Secure Flight, the pre-screening system for domestic passengers, uses a lot less information and has shorter retention periods for cleared passengers (DHS 2010b).[9] This double standard is something Europe is definitely not exempt from, see for example the treatment of third country nationals in immigration matters (Guild 2009: 116-128). Finally, the debate usually excludes the downsides of risk analysis and profiling (Ericson 2006), a function of the widespread belief in technological fixes.

Providing sufficient recognition to all those affected by the decisions is an important step in civilising security practices (Loader and Walker 2007: 220-222). After all, what critics of PNR transfers attacked was not the provision of security measures as such, but they way in which it was done: With insufficient public justifications, in a non-transparent process, without clear evidence for their usefulness, without sufficiently strict legal safeguards. None of them would have denied that aviation security is an important objective. If the case for the use of PNR was made with sound reasoning, respect for the rights of the passengers, and recognition of their interests, that is with some preconditions for a democratic governance of security (Loader and Walker 2007: 215-233), then a lot of the criticism would go away. Dragging the debate out into the public could ensure that the security apparatus is sufficiently controlled. One forum to provide such control is the European Parliament, which now has the power to make a real difference.

9 Secure Flight checks basic passenger data (full name, sex, date of birth) against a range of watch lists to refer passengers to secondary screening or prevent them from boarding if a match is identified. Data on passengers that are cleared is kept for seven days (DHS 2008c): 13-14). International flights are checked against Secure Flight additionally to the analysis carried out under PNR agreements.

Bibliography

9/11 Commission 2004: *Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington, D.C.: Government Printing Office.

Abrahamsen, Rita, and Michael C. Williams 2009: "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3(1):1-17.

Abrutyn, Seth 2009: "Toward a General Theory of Institutional Autonomy." *Sociological Theory* 27(4):449-465.

Aldrich, Richard J. 2004: "Transatlantic intelligence and security cooperation." *International Affairs* 80(4):731-753.

Allison, Graham, and Philipp Zelikow 1999: *Essence of Decision: Explaining the Cuban Missile Crisis*. 2nd edition. New York: Longman.

American Civil Liberties Union 2007: "EU-US PNR agreement in light of "Automated Targeting System"" Letter to the European Parliament, January 9 2007.

Amoore, Louise 2006: "Biometric borders: Governing mobilities in the war on terror." *Political Geography* 25(3):336-351.

Andreas, Peter, and Ethan Nadelmann 2006: *Policing the Globe*. Oxford: Oxford University Press.

Aradau, Claudia, and Rens van Munster 2009: "Exceptionalism and the 'War on Terror': Criminology Meets International Relations." *British Journal of Criminology* 49(5):686-701.

Article 29 Data Protection Working Party 2002: "Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States." *Working Paper 66.*

Article 29 Data Protection Working Party 2003a: "Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data." *Working Paper* 78.

Article 29 Data Protection Working Party. 2003b: "Opinion of the European Data Protection Authorities on the Transfer of Passengers' Data to the United States."

Article 29 Data Protection Working Party 2004a: "Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)." *Working Paper* 87.

Article 29 Data Protection Working Party. 2004b: "Opinion 6/2004 on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the 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." *Working Paper* 95.

Article 29 Data Protection Working Party 2006: "Opinion 7/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement." *Working Paper* 138.

Article 29 Data Protection Working Party 2007a: "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." *Working Paper* 145.

Article 29 Data Protection Working Party 2007b: "Opinion 5/2007 on the follow-up 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 concluded in." *Working Paper 138*.

Article 29 Data Protection Working Party 2010: "Opinion 7 / 2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries" *Working Paper* 178.

Austin, John L. 1977. *How to do things with words*. Cambridge: Harvard University Press.

Aviation And Transport Security Act 2001: "An Act to improve aviation security, and for other purposes" *Public Law* 107–71, 107th Congress

Baker, Stewart A. 2003: "Testimony before the National Commission on Terrorist Attacks Upon the United States" December 8, 2003.

Baker, Stewart A. 2010: *Skating on Stilts - Why We Aren't Stopping Tomorrow's Terrorism*. Stanford: Hoover Institution Press.

Balzacq, Thierry 2005: "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11(2):171-201.

Balzacq, Thierry 2008: "The policy tools of securitization: Information exchange, EU foreign and interior policies" *Journal of Common Market Studies* 46(1):75-100.

Balzacq, Thierry 2009: "Constructivism and Securitization Studies" Pp. 56-72 in *Handbook of Security Studies*, edited by Myriam Dunn Cavelty and Victor Mauer. London: Routledge.

Barthwal-Datta, Monika 2009: "Securitising Threats without the State: A Case Study of Misgovernance as a Security threat in Bangladesh" *Review of International Studies* 35(2):277-300.

Basaran, Tugba 2008: "Security, Law, Borders: Spaces of Exclusion" *International Political Sociology* 2(4):339-354.

Behnke, Andreas 2000: "The Message or the Messenger? Reflections on the Role of Security Experts and the Securitization of Political Issues" *Cooperation and Conflict* 35(1):89-105.

Bennett, Colin J., and Charles Raab 2006: *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press.

Bigo, Didier, and Anastassia Tsoukala 2008: "Understanding (in)security" Pp. 1-9 in *Terror, Insecurity and Liberty - Illiberal practices of liberal regimes after 9/11*, edited by Didier Bigo and Anastassia Tsoukala. Abingdon: Routledge.

Bigo, Didier. 1992: *L'Europe des polices et de la sécurité intérieure.* Brussels: Editions Complexes.

Bigo, Didier. 1996: *Polices en Reseaux: L'Experience Europénne*. Paris: Presses de Sciences Po.

Bigo, Didier. 2000: "When Two Become One: Internal and External Securitisations in Europe" Pp. 171-204 in *International Relations Theory and the Politics of European Integration*, edited by Morten Kelstrup and Michael C. Williams. London: Routledge.

Bigo, Didier 2002: "Security and Immigration: Toward a Critique of the Governmentality of Unease" *Alternatives* 27(Special Issue):63-92.

Bigo, Didier 2006: "Security, Exception, Ban and Surveillance" Pp. 46-68 in *Theorizing Surveillance - The panopticon and beyond*, edited by David Lyon. Cullompton: Willan.

Bigo, Didier 2007: "Mobility Controls and New Technologies." Pp. 9-14 in *Are you who you say you are? The EU and Biometric Borders*, edited by Juliet Lodge. Nijmegen: Wolf Legal.

Bigo, Didier 2008a: "EU Police Cooperation: National Sovereignty Framed by European Security?" Pp. 91-108 in *Security versus Justice? Police and Judicial Cooperation in the European Union*, edited by Elspeth Guild and Florian Geyer. Aldershot: Ashgate.

Bigo, Didier 2008b: "Globalized (in)Security: The Field and the Ban-opticon." Pp. 5-49 in *Illiberal Practices in Liberal Regimes*, edited by Didier Bigo and Anastassia Tsoukala. Paris: L'Harmattan.

Bigo, Didier 2008c: "International Political Sociology." Pp. 116-128 in *Security Studies - An Introduction*, edited by Paul D. Williams. Abingdon: Routledge.

Bolkestein, Frits 2003a: "EU/US talks on transfers of airline passengers' personal data" Address to European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Brussels, 9th September 2003.

Bolkestein, Frits 2003b: "EU/US talks on transfers of airline passengers' personal data" Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market, Brussels, 1st December 2003.

Bolkestein, Frits 2003c: "EU/US talks on transfers of airline passengers' personal data" Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market, Strasbourg, 16th December 2003.

Bolkestein, Frits 2003d: "Letter to DHS Secretary Tom Ridge".

Bundesverfassungsgericht 2010: *1 BvR 256/08*, 02.03.2010.

Buzan, Barry 1997: "Rethinking Security after the Cold War." *Cooperation and Conflict* 32(1):5-28.

Buzan, Barry, and Ole Wæver 2003: *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.

Buzan, Barry, and Ole Wæver 2009: "Macrosecuritisation and security constellations: reconsidering scale in securitisation theory" *Review of International Studies* 35(2):253-276.

Buzan, Barry, Ole Wæver, and Jaap De Wilde 1998: *Security: A New Framework for Analysis*. Boulder: Lynne Rienner.

c.a.s.e. Collective 2006: "Critical Approaches to Security in Europe: A Networked Manifesto" *Security Dialogue* 37(4):443-487.

CHALLENGE 2007: "Mapping of the European Security Agencies" available at: http://www.libertysecurity.org/IMG/pdf_Mapping_30.11.2007.pdf, last access: 12/10/2010.

Chertoff, Michael 2006a: "A Tool We Need to Stop the Next Airliner Plot" *The Washington Post* August 29,2006.

Chertoff, Michael 2006b: "Speech at the National Lawyers' Conference, November 16th 2006" *Engage* 8(2):67-71.

Chertoff, Michael 2006c: "Testimony before the Senate Committee on Homeland Security and Governmental Affairs September 12, 2006" Washington, D.C.: US Senate.

Chertoff, Michael 2007: "Letter to the European Parliament, May 14 2007"

Ciută, Felix 2009: "Security and the Problem of Context: A Hermeneutical Critique of Securitisation Theory" *Review of International Studies* 35(2):301-326.

Committee On Civil Liberties Justice And Home Affairs 2006: "Report with a proposal for a European Parliament recommendation to the Council on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime" *European Parliament Document* A6-0252/2006 Final.

Council of the European Union 2003: "AVIATION - New legal requirements by US on 'Advanced Passenger Information System' (APIS) and 'Passenger Name Records' (PNR) = Exchange of views on the position of the Member States. Discussion by Working Party on Aviation on 28 January 2003." *Council Document* 6051/03.

Council of the European Union 2004a: "Council Decision 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 - Approval of a Reply to the Letter of Mr Pat Cox, President of the European Parliament" *Council Document* 9860/04.

Council of the European Union 2004b: "Council Directive 2004/82/EC of 29 April 2004 on the Obligation of Carriers to Communicate Passenger Data" *Official Journal of the European Union* L 261:24-27.

Council of the European Union 2004c: “Letter to Patrick Cox 25.03.2004” *European Parliament Document* EP-PE_LTA(2004)004597_FR.

Council of the European Union 2004d: “Preparation of the 35th ICAO Assembly - An International Framework for the Transfer of Passenger Name Record (PNR) Data - Confirmation of text - decision on the use of the written procedure.” *Council Document* 12397/1/04.

Council of the European Union 2006a: “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” *Council Document* 13668/06.

Council of the European Union 2006b: “Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament - Information meeting with the participation of the national parliaments of the Member States: "The consequences of the judgment of the European Court of Justice on the 'Passenger Name Records' (PNR) at the national and European level (Joined Cases C-317/04 and C-318/04)"” *Council Document* 10925/06.

Council of the European Union 2006c: “Termination of the 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” *Council Document* 10613/06.

Council of the European Union 2006d: “Council adopts decision on signature of Agreement with the United States on the continued use of PNR data.” *Council Document* 14006/06.

Council of the European Union 2006e: “Council Decision 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 Unit.” *Official Journal of the European Union* L 298/27.

Council of the European Union 2006f: “Plenary session of the European Parliament in Brussels, 11 October 2006 - Council and Commission statements - Use of passenger data (PNR).” *Council Document* 13991/06.

Council of the European Union 2007: “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 - Letter on confidentiality of negotiation” *Council Document* 12309/07.

Council of the European Union 2009: “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 – Declarations made in accordance with Article 24(5) TEU - State of Play” *Council Document* 5311/1/09.

Council of the European Union 2010a: “EU external strategy on Passenger Name Record (PNR) data - Handling of draft negotiation mandates for PNR Agreements with Canada, the United States of America and Australia.” *Council Document* 13986/10.

Council of the European Union 2010b: “Press Release 3051st Council Meeting Justice and Home Affairs, Brussels, 2-3 December 2010.” *Council Document* 16918/10.

Cox, Pat 2004: “Letter to the Council Presidency” *Council Document* 9614/04.

Curry, Michael R. 2002: “The Profiler’s Question and the Treacherous Traveler: Narratives of Belonging in Commercial Aviation” *Surveillance & Society* 1(4):475-499.

De Busser, Els 2009: “Purpose Limitation in EU-US Data Exchange in Criminal Matters: the Remains of the Day” Pp. 163-201 in *Readings On Criminal Justice, Criminal Law & Policing Vol. 2*, edited by Marc Cools. Antwerp: Maklu.

De Goede, Marieke 2008: “The Politics of Preemption and the War on Terror in Europe” *European Journal of International Relations* 14(1):161-185.

Deflem, Mathieu 2000: “Bureaucratization and social control: Historical foundations of international police cooperation.” *Law and Society Review* 34(3):739–778.

Deflem, Mathieu 2002: *Policing World Society*. Oxford: Oxford University Press.

DHS2003a: "Press Release 09/11/03: Remarks of Nuala O'Connor Kelly, Chief Privacy Officer, Before the 25th International Conference of Data Protection and Privacy Commissioners."

DHS2003b: "Press Release 09/16/03: Remarks by Secretary Tom Ridge to the Council for Excellence in Government"

DHS2003c: "Press Release 12/16/03 Homeland Security and European Commission Reach Agreement on PNR Data"

DHS2004a: "Press Release 02/13/04: CAPPS II: Myths and Facts."

DHS2004b: "Press Release 02/13/04: Fact Sheet: CAPPS II at a Glance."

DHS2004c: "Press Release 05/17/04: Statement by Homeland Security Secretary Tom Ridge on European Commission Decision."

DHS2004d: "Press Release 05/28/04: DHSnd EU Sign Agreement to Allow Collection of Passenger Data."

DHS2004e: "Press Release 06/24/04: Remarks by Deputy Secretary of Homeland Security James Loy at the German Marshall Fund."

DHS 2004f: "Press Release 07/08/04: Background Briefing by Senior Intelligence Officials."

DHS 2004g: "Press Release 09/13/04: Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University 'Transatlantic Homeland Security Conference'."

DHS 2004h: "Press Release 11/22/04: Transcript of Under Secretary Asa Hutchinson and European Union Director-General Jonathan Faull at Press Conference."

DHS 2004i: "Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP)." *Federal Register* 69(131):41543-41547.

DHS 2005a: “A Report Concerning Passenger Name Record Information Derived from Flights between the U.S. and the European Union.” Privacy Office U.S. Department of Homeland Security.

DHS 2005b: “Department Six-Point Agenda.” available at: http://www.dhs.gov/xabout/history/editorial_0646.shtm. Last access: 13/11/2010.

DHS 2005c: “Press Release 03/16/05: Remarks for Secretary Michael Chertoff U.S. Department of Homeland Security George Washington University Homeland Security Policy Institute.”

DHS 2005d: “Press Release 04/13/05: Testimony by Secretary Michael Chertoff Before the House Homeland Security Committee.”

DHS 2005e: “Press Release 05/19/05: Transcript of Secretary of Homeland Security Michael Chertoff at the Center for Strategic and International Studies.”

DHS 2005f: “Press Release 05/23/05: Remarks by Secretary of Homeland Security Michael Chertoff at the German Marshall Fund and European Policy Centre.”

DHS 2005g: “Press Release 07/13/05: Homeland Security Secretary Michael Chertoff Announces Six-Point Agenda for Department of Homeland Security.”

DHS 2005h: “Press Release 07/14/05: Testimony of Secretary of Homeland Security Michael Chertoff Before the Senate Homeland Security and Governmental Affairs Committee.”

DHS 2005i: “Press Release 07/19/05: Statement of Secretary Michael Chertoff U.S. Department Of Homeland Security Before the United States Senate Committee On Commerce, Science and Transportation.”

DHS 2006a: “Press Release 01/17/06: Fact Sheet: Secure Borders and Open Doors in the Information Age.”

DHS 2006b: “Press Release 03/07/06: Remarks by the Secretary of Homeland Security Michael Chertoff at a Data Privacy and Integrity Meeting.”

DHS 2006c: “Press Release 09/30/06: Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Agreement with European Union.”

DHS 2006d: “Press Release 11/06/06: Remarks by Attorney General Alberto Gonzales, Secretary of Homeland Security Michael Chertoff, Vice President of the European Union Franco Frattini, Finland Minister of Interior Kari Rajamaki, Finland Minister of Justice Leena Luhtanen.”

DHS 2007a: “Press Release 05/15/07: Secretary Chertoff’s Remarks to European Parliament.”

DHS 2007b: “Press Release 07/05/07: Statement by Secretary Michael Chertoff on Passenger Name Record Data.”

DHS 2007c: “Press Release 07/26/07: Statement By Homeland Secretary Michael Chertoff On A New Agreement With The European Union For Passenger Name Record Data Sharing.”

DHS 2007d: “Press Release 08/09/07: DHS Announces Predeparture Screening of International Passengers and First Step Toward Secure Flight.”

DHS 2007e: “Press Release 09/05/07: Testimony of Secretary Michael Chertoff before the House Committee on Homeland Security.”

DHS 2007f: “Press Release 09/10/07: Testimony of Secretary Michael Chertoff Before the Senate Committee on Homeland Security "Confronting the Terrorist Threat to the Homeland: Six Years After 9/11".”

DHS 2007g: “Press Release 11/15/07: Remarks by Homeland Security Secretary Michael Chertoff at the Eighth Annual U.S. Customs and Border Protection 2007 Trade Symposium.”

DHS 2007h: “Press Release 12/07/07: Fact Sheet: Select Department of Homeland Security 2007 Achievements.”

DHS 2008a. “A Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and the European Union.” Privacy Office U.S. Department of Homeland Security.

DHS 2008b. *Information Sharing Strategy*. U.S. Department of Homeland Security.

DHS 2008c: “Privacy Impact Assessment for the Secure Flight Program.” Privacy Office U.S. Department of Homeland Security.

DHS 2010a: “DHS Response to the European Commission’s Report on the Joint Review of the U.S. - EU Passenger Name Records Agreement.” Letter to the European Commission.

DHS 2010b: “Press Release 11/30/10: DHS Achieves Major Aviation Security Milestone One Month Ahead of Schedule.”

DHS 2010c: “Update to the 2008 report concerning passenger name record information derived from flights between the U.S. and the European Union.” Privacy Office U.S. Department of Homeland Security.

Dillon, Michael 2008: “Underwriting Security.” *Security Dialogue* 39(2-3):309-332.

Elias, Bartholomew 2010: *Airport and Aviation Security - U.S. Policy and Strategy in the Age of Global Terrorism*. Boca Raton: CRC Press.

Enhanced Border Security and Visa Entry Reform Act 2002: “An Act to Enhance the Border Security of the United States, and for Other Purposes.” *Public Law* 107-173, 107th Congress.

Ericson, Richard V. 2006. “Ten Uncertainties of Risk-Management Approaches to Security.” Canadian Journal of Criminology and Criminal Justice 48(3):345-357.

Ericson, Richard V. 2007. *Crime in an Insecure World*. Cambridge: Polity.

Eriksson, Johan, and Mark Rhinard 2009: “The Internal-External Security Nexus: Notes on an Emerging Research Agenda.” *Cooperation and Conflict* 44:243-267.

Eriksson, Johan 1999: “Observers or Advocates?: On the Political Role of Security Analysts.” *Cooperation and Conflict* 34(3):311-330.

EU Observer 2008: “EU endorses idea of collecting air passenger data.” available at http://euobserver.com/9/26539?print=1. Last access 07/10/2010.

EU-CA PNR Agreement. 2006. "Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data." *Official Journal of the European Union* L 82/15.

EU-US Joint Declaration on Aviation Security 2010: "EU-US Joint Declaration on Aviation Security, Toledo, 21 January 2010." available at http://www.eu2010.es/en/documentosynoticias/otrasdeclarac/jaieuusa.html. Last access 12/12/2010.

EU-USA PNR Agreement 2004: "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." *Official Journal of the European Union* L 183/84.

EU-USA PNR Agreement. 2006: "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." *Official Journal Of The European Union* L 298/29.

EU-USA PNR Agreement 2007: "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)." *Official Journal of the European Union* L 204/18.

European Commission 2003: "Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach." *Commission Document* COM(2003)826 final.

European Commission 2004a: "Commission decision 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 (2004/535/EC)." *Official Journal of the European Union* L 235/11.

European Commission 2004b: "Commission Staff Working Paper 'An EC-U.S. Agreement on Passenger Name Record (PNR)'." *Commission Document* SEC(2004)81.

European Commission 2004c: “Commission staff working paper: Preparation of the 35th ICAO assembly - An international framework for the transfer of Passenger Name Record (PNR) Data” *Commission Document* SEC(2004)1138.

European Commission 2005: “Commission Staff Working Paper on the joint review of the implementation by the U.S. Bureau of Customs and Border Protection of the Undertakings set out in Commission Decision 2004/535/EC of 14 May 2004 [redacted version].” *Commission Document* COM(2005) final.

European Commission 2006a: “Note à l’attention des membres de la commission” *Commission Document* SEC(2006)766.

European Commission 2006b: “Recommendation from the Commission to the Council to authorise opening of negotiations for an agreement with the United States of America on the use of Passenger Name Recors (PNR) data to prevent and combat terrorism and related transnational crime, as we.”

European Commission 2006c: “Recommendation from the Commission to the Council to authorise opening of negotiations for an agreement with the United States of America on the use of Passenger Name Recors (PNR) data to prevent and combat terrorism and related transnational crime, including organised crime.” *Commission Document* SEC(2006)812 final.

European Commission 2007a: “Commission Staff Working Document: Accompanying document to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Summary of the Impact Assessment.” *Commission Document* SEC(2007)1422.

European Commission 2007b: “Commission Staff Working Document: Accompanying document to the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes: Impact Assessment.” *Commission Document* SEC(2007)1453.

European Commission 2007c: “proposition de decision-cadre du conseil relative a l'utilisation des donnees des dossiers passagers (pnr) a de fins repressifs.” *Commission Document* COM(2007)654.

European Commission 2010a: "Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries." *Commission Document* COM(2010)492 final.

European Commission 2010b: "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 Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)." *Council Document* 8506/10.

European Commission / US Customs 2003: "European Commission / US Customs Talks on PNR Transmission Joint Statement." Brussels, 17/18 February 2003.

European Court of Human Rights. 2008: "Case of S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04)) Judgment, Strasbourg 4 December 2008."

European Court of Justice. 2006: "Judgment in cases C-317/04 and C-318/04." *Official Journal of the European Union* C 178/1.

European Data Protection Supervisor. 2008: "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 (2008/C 110/01)." *Official Journal of the European Union* C 110/1.

European Parliament. 2003a: "Debates: Transfer of personal data by airlines to the US imigration service, 12 March 2003, Strasbourg."

European Parliament 2003b: "European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights." *European Parliament Document* P5_TA(2003)0097.

European Parliament 2003c: "European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flights: state of negotiations with the USA." *European Parliament Document* P5_TA(2003)0429.

European Parliament 2004a: "Action brought on 27 July 2004 by the European Parliament against the Council of the European Union (Case C-317/04)." *Official Journal of the European Union* C 228/31.

European Parliament 2004b: "Action brought on 27 July by the European Parliament against the Commission of the European Communities (Case C-318/04)." *Official Journal of the European Union* C 228/32.

European Parliament 2004c: "Debates: Council and Commission statements on transtlantic relations, 21 April 2004, Strasbourg."

European Parliament 2004d: "Debates: EC-USA agreement on PNR, 20 April 2004, Strasbourg."

European Parliament 2004e: "Debates: Obligation of carriers to communicate passenger data, 31 March 2004, Strasbourg."

European Parliament 2004f: "Debates: Passenger Name Record Data, 19 April 2004, Strasbourg."

European Parliament 2004g: "Debates: Protection of personal data of air passengers, 29 March 2004, Strasbourg."

European Parliament 2004h: "European Parliament resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection." *European Parliament Document* 2004/2011(INI).

European Parliament 2004i: "Report on the proposal for a Council decision 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." *European Parliament Document* A5-0271/2004 final.

European Parliament 2006a: "Debate: Data Protection, 13 December 2006, Strasbourg."

European Parliament 2006b: "Debates: Protection of Personal Data, 13 June 2006, Strasbourg."

European Parliament 2006c: “Debates: Use of Passenger Data (PNR), 11 October 2006, Brussels.”

European Parliament 2006d: “Debates: Use of passenger personal data Agreement with the USA on the use of Passenger Name Record data, 7 September 2006, Strasbourg.”

European Parliament 2006e: “European Parliament recommendation to the Council on the negotiations for an agreement with the United States of America on the use of passenger name records (PNR) data to prevent and combat terrorism and transnational crime, including organised crime” *European Parliament Document* P6_TA(2006)0354.

European Parliament 2006f: “Press Release 13 September 2006: PNR: Frattini updates MEPs on talks with USA.”

European Parliament 2006g: “Press Release 14 July 2006: MEPs want to be present at negotiations of passenger data agreement with USA.”

European Parliament 2007a: “Debates: Explanation of Votes, 12 July 2007, Strasbourg.”

European Parliament 2007b: “Debates: Fight against Terrorism, 5 September 2007, Strasbourg.”

European Parliament 2007c: “Debates: New PNR Agreement SWIFT, 31 January 2007, Brussels.”

European Parliament 2007d: “Debates: PNR Agreement with the United States, 09 July 2007, Strasbourg.”

European Parliament 2007e: “Debates: Transatlantic Relations, 25 April 2007, Strasbourg.”

European Parliament 2007f: “European Parliament resolution of 12 July 2007 on the PNR agreement with the United States of America.” *European Parliament Document* P6_TA-PROV(2007)0347.

European Parliament 2010: “Resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada.” *European Parliament Document* P7_TA-PROV(2010)0144.

European Parliament Legal Service 2004: “Proposition de décision du Conseil concernant la conclusion d’un accord entre la Communauté européenne et les Etats-Unis d'Amerique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières due ministère américaine de la sécurité intérieur” *European Parliament Document* D(2004)14756.

Forsberg, Tuomas, and Graeme P Herd 2006: *Divided West - European Security and the Transatlantic Relationship*. Malden: Blackwell.

Freedman, Lawrence 2005: “The Transatlantic Agenda: Vision and Counter-Vision.” *Survival* 47(4):19-38.

Gandy, Oscar H. 2003: “Data Mining and Surveillance in the Post-9/11 Environment.” Pp. 26-41 in *The Intensification of Surveillance*, edited by Kristie Ball and Frank Webster. London: Pluto.

Gandy, Oscar H. 2006: “Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment.” Pp. 363-384 in *The New Politics of Surveillance and Visibility*, edited by Kevin D. Haggerty and Richard V. Ericson. Toronto: University of Toronto Press.

Garfinkel, Harold. 1967: *Studies in Ethnomethodology*. Englewood Cliffs: Prentice-Hall.

Gerspacher, Nadia, and Benoît Dupont 2007: “The Nodal Structure of International Police Cooperation: An Exploration of Transnational Security Networks.” *Global Governance* 13(2):347- 364.

González Fuster, Gloria, and Paul de Hert 2007: "PNR and Compensation - How to Bring Back the Proportionality Criterion." Pp. 101-109 in *Are you who you say you are? The EU and Biometric Borders*, edited by Juliet Lodge. Nijmegen: Wolf Legal.

González Fuster, Gloria, Serge Gutwirth, and Erika Ellyne 2010: "Profiling in the European Union: A high-risk practice." *INEX Policy Brief* 10.

Guild, Elspeth, and Evelien Brouwer 2006: "The Political Life of Data." *CEPS Policy Brief* 109.

Guild, Elspeth, Sergio Carrera, and Thierry Balzacq 2008: "The Changing Dynamics of Security in an Enlarged European Union." *CHALLENGE Liberty and Security Research Paper* 12.

Guild, Elspeth 2007: "Inquiry into the EU-US Passenger Name Record Agreement." *CEPS Policy Brief* 125.

Guild, Elspeth 2009. *Security and Migration in the 21st Century*. Cambridge: Polity.

Guild, Elspeth 2010: "Global Data Transfers : The Human Rights Implications." *INEX Policy Brief*.

Guzik, Keith 2009: "Discrimination by Design: predictive data mining as security practice in the United States 'war on terrorism'." *Surveillance & Society* 7(1):1-17.

Hailbronner, Kay, Vagelis Papakonstantinou, and Marcel Kau 2008: "The Agreement on Passenger-Data Transfer (PNR) and the EU-US Cooperation in Data Communication." *International Migration* 46(2):187-197.

Hansen, Lene 2000: "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School." *Millennium - Journal of International Studies* 29(2):285-306.

Hansen, Lene 2006: *Security as Practice - Discourse Analysis and the Bosnian War*. London: Routledge.

Have, Paul ten 2002: *Understanding Qualitative Research and Ethnomethodology*. London: Sage.

Hobbing, Peter 2008: "Tracing Terrorists : The EU-Canada Agreement in PNR Matters." C*EPS Special Report September* 2008.

House of Lords 2007: *The EU/US Passenger Name Record (PNR) Agreement – Report with Evidence.* London: Stationery Office.

House of Lords 2008: *The Passenger Name Record (PNR) Framework Decision - Report with Evidence*. London: Stationery Office.

Hudson, Valerie M. 2007: *Foreign Policy Analysis: Classic and Contemporary Theory*. Lanham: Rowman & Littlefield.

Huysmans, Jef, and Alessandra Buonfino 2008: "Politics of Exception and Unease: Immigration, Asylum and Terrorism in Parliamentary Debates in the UK." *Political Studies* 56(4):766-788.

Huysmans, Jef 2002: "Defining Social Constructivism in Security Studies: The Normative Challenge of Writing Security." *Alternatives* 27(1):41-62.

Huysmans, Jef 2006. *The politics of insecurity: fear, migration and asylum in the EU*. London: Routledge.

ICAO 2004: "Airline Reservation System and Passenger Name Record (PNR) Access by States" *Working Paper* FAL/12-WP/74.

ICAO 2008: "Recommendations Relating to ICAO's Best Practices Relating to Passenger name Record (PNR) (Presented by the International Air Transport Association (IATA)." *Working Paper* FALP/5-WP/26.

ICAO 2010: "Report of the Advance Passenger Information / Passenger Name Record Working Group." *Working Paper* FALP/6-WP/5.

Intelligence Reform and Terrorism Prevention Act 2004: "An Act to reform the intelligence community and the intelligence and intelligence-related activities of the United States Government, and for other purpose." Public Law 108-458, 108th Congress.

Kaunert, Christian 2007: "'The Construction of a European Interest in Foreign Policy': The Area of Freedom, Security and Justice and EU-US Counter-Terrorism Relations." *Paper presented at the 2007 Pan-European Conference in Turin, Italy, 12-15 September 2007.*

Koc-Menard, Sergio 2009: "Trends in Terrorist Detection Systems." *Journal Of Homeland Security And Emergency Management* 6(1):1-13.

Koslowski, Rey 2006: "Border and transportation security in the transatlantic relationship." Pp. 89-105 in *Transatlantic Homeland Security - Protecting society in the age of catastrophic terrorism*, edited by Anja Dalgaard-Nielsen and Daniel S. Hamilton. London: Routledge.

Lahav, Gallya 2008: "Mobility and Border Security: The U.S. Aviation System, The State, and the Rise of Public-Private Partnerships." Pp. 77-104 in *Politics at the Airport*, edited by Mark B. Salter. Minneapolis: University of Minnesota Press.

Loader, Ian, and Neill Walker 2007: *Civilizing Security.* Cambridge: Cambridge University Press.

Lyon, David 2001: *Surveillance Society - Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, David 2006: "Airport Screening, Surveillance, and Social Sorting: Canadian Responses to 9 / 11 in Context." *Canadian Journal of Criminology and Criminal Justice* 48(3):397-411.

Lyon, David 2007: *Surveillance Studies - An Overview.* Cambridge: Polity.

Lyon, David 2008: "Filtering Flow, Friends and Foes: Global Surveillance." Pp. 29-50 in *Politics at the Airport*, edited by Mark B. Salter. Minneapolis: University of Minnesota Press.

Mahncke, Dieter, Wyn Rees, and Wayne Thompson: 2004. *Redefining Transatlantic Security Relations - The Challenge of Change*. Manchester: Manchester University Press.

Martin, Lauren, and Stephanie Simon. 2008: “A Formula for Disaster: The Department of Homeland Security’s Virtual Ontology.” *Space and Polity* 12(3):281-296.

McSweeney, Bill 1996: “Identity and security: Buzan and the Copenhagen school.” *Review of International Studies* 22(1):81-93.

Mitsilegas, Valsamis 2005: “Controlling Foreigners, Passengers, Citizens: Surveillance and Counter-Terrorism.” *Cultures & Conflits* 58(Summer):155-182.

Mitsilegas, Valsamis 2008: “Coopération antiterroriste États-Unis/Union européenne: l’entente cordiale.” Pp. 118-130 in *Au nom du 11 Septembre... les démocraties à l’épreuve de l'antiterrorisme*, edited by Didier Bigo, Laurent Bonelli, and Thoms Deltombe. Paris: La Découverte.

Mitsilegas, Valsamis 2009: “Borders, Security, and Transatlantic Cooperation in the Twenty-First Century: Identity and Privacy in an Era of Globalized Surveillance.” Pp. 148-166 in *Immigration Policy and Security - U.S, European, and Commonwolth Perspectives*, edited by Terri E. Givens, Gary P. Freeman, and David L. Leal. London: Routledge.

Müller-Wille, Björn 2008: “The Effect of International Terrorism on EU Intelligence Co-operation.” *Journal of Common Market Studies* 46(1):49-73.

Munster, Rens van 2007: “Review Essay: Security on a Shoestring: A Hitchhiker’s Guide to Critical Schools of Security in Europe.” *Cooperation and Conflict* 42(2):235-243.

Mythen, Gabe, and Sandra Walklate 2008: “Terrorism, Risk and International Security: The Perils of Asking ‘What If?’” *Security Dialogue* 39(2-3):221-242.

Neocleous, Mark 2006: “The Problem With Normality: Taking Exception to "Permanent Emergency".” *Alternatives* 31(2):191-213.

Ntouvas, Ioannis 2007: “Air Passenger Data Transfer to the USA: the Decision of the ECJ and the latest developments.” *International Journal of Law and Information Technology* 16(1):73-95.

O'Malley, Pat. 2006: "Risks, Ethics, and Airport Security." *Canadian Journal of Criminology and Criminal Justice* 48(3):413-421.

Oberhuber, Florian, and Michal Krzyzanowski 2008: "Discourse Analysis and Ethnography." Pp. 182-203 in *Qualitative Discourse Analysis in the Social Sciences*, edited by Ruth Wodak and Michal Krzyzanowski. Houndmills: PalgraveMacMillan.

ORF Futurezone 2008: "Frattini will PNR-Erfassung durchpeitschen." avaliable at http://futurezone.orf.at/stories/252094/. Last access: 20/07/2010.

Papakonstantinou, Vagelis, and Paul de Hert 2009: "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic." *Common Market Law Review* 46(3):885-919.

Peoples, Columba, and Nick Vaughan-Williams 2010. *Critical Security Studies - An Introduction*. Abingdon: Routledge.

Rees, Wyn 2006: "International Cooperation in Counter-Terrorism – The Transatlantic Dimension and Beyond." Pp. 113-127 in *International Terrorism – A European Response to a Global Threa*, edited by Dieter Mahncke and Jörg Monar. Brussels: P.I.E. Pete Lang.

Sales, Nathan Alexander 2002: "Share and share alike?" *The George Washington Law Review* 78(2):279-352.

Salter, Mark B. 2006: "The Global Visa Regime and the Political Technologies of the International Self: Borders, Bodies, Biopolitics." *Alternatives* 31(1):167-189.

Salter, Mark B. 2008a: "Imagining Numbers: Risk, Quantification, and Aviation Security." *Security Dialogue* 39(2-3):243-266.

Salter, Mark B. 2008b: "Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority." *Journal of International Relations and Development* 11(4):321-349.

Salter, Mark B. 2008c: "The Global Airport - Managing Space, Speed, and Security." Pp. 1-28 in *Politics at the Airport*, edited by Mark B. Salter. Minneapolis: University of Minnesota Press.

Sheptycki, James 2007: “Criminology and the Transnational Condition: A Contribution to International Political Sociology.” *International Political Sociology* 1(4):391-406.

Stentzel, Rainer. 2010: “Datenschutz zwischen Utopie und Anpassung. Die politische Debatte um den polizeilichen Datenaustausch mit den USA.” *Zeitschrift für Außen- und Sicherheitspolitik* 3(2):137-148.

Stritzel, Holger 2007: “Towards a Theory of Securitization: Copenhagen and Beyond.” *European Journal of International Relations* 13(3):357-383.

Sweet, Kathleen M. 2009: *Aviation and Airport Security - Terrorism and Safety Concerns*. Boca Raton: CRC.

Tanaka, Hiroyuki, Rocco Bellanova, Susan Ginsburg, and Paul de Hert: 2010. *Transatlantic Information Sharing at a Crossroads*. Migration Policy Institute: Washington, D.C.

Thomson, Mary E., Dilek Onkal, Ali Avcioğlu, and Paul Goodwin. 2004: “Aviation risk perception: a comparison between experts and novices.” *Risk analysis* 24(6):1585-95.

US House of Representatives 2001a: “Aviation Security Act.” *Congressional Record* 147(House): 7754.

US House of Representatives 2001b: “Conference Report on S. 1447 Aviation and Transportation Security Act.” *Congressional Record* 147(House):8300.

US Senate 2001: “Aviation and Transportation Security Act - Conference Report.” *Congressional Record* 147(Senate):11974.

Volpi, Frédéric 2007: “Constructing the "Ummah" in European Security: Between Exit, Voice and Loyalty.” *Government and Opposition* 42(3):451-470.

Vuori, Juha A. 2008: “Illocutionary Logic and Strands of Securitization: Applying the Theory of Securitization to the Study of Non-Democratic Political Orders.” *European Journal of International Relations* 14(1):65-99.

Walsh, James I. 2006: “Intelligence-sharing in the European Union: Institutions are not enough.” *Journal of Common Market Studies* 44(3):625-43.

Walt, Stephen M. 1991: “The Renaissance of Security Studies.” *International Studies* 35(2):211-239.

Whitman, James Q. 2004: “The Two Western Cultures of Privacy: Dignity versus Liberty.” *Yale Law Journal* 113:1151-1221.

Williams, Michael C. 2003: “Words, images, enemies: securitization and international politics.” *International Studies Quarterly* 47(4):511–531.

Wodak, Ruth. 2008: “Introduction: Discourse Studies - Important Concepts and Terms.” Pp. 1-29 in *Qualitative Discourse Analysis in the Social Sciences*, edited by Ruth Wodak and Michal Krzyzanowski. Houndmills: PalgraveMacMillan.