THIS PROJECT IS FUNDED
BY THE EUROPEAN UNION

IMPROVING US AND EU IMMIGRATION SYSTEMS

Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals

By Paul De Hert and Rocco Bellanova

RSCAS European University Institute
Robert Schuman Centre for Advanced Studies
MIGRATION POLICY INSTITUTE

TRANSATLANTIC COOPERATION ON TRAVELERS' DATA PROCESSING:

From Sorting Countries to Sorting Individuals

By Paul De Hert and Rocco Bellanova

March 2011

Acknowledgments

This report was produced for Pilot Projects on Transatlantic Methods for Handling Global Challenges in the European Union and the United States, a project funded by the European Commission. The project is conducted jointly by the Migration Policy Institute and the European University Institute. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union.

The authors would like to thank Madeleine Sumption for her advice and accurate and patient editing. They would also like to thank Leda Bargiotti for her comments and remarks. The authors alone are responsible for any errors or inaccuracies.

Cover Photo: Modified version of "American Flag" (104660440) and "Flag of the European Union" (WFL_074) - Photos.com
Cover Design: Burke Speaker, MPI
Typesetting: April Siruno, MPI

Suggested citation: De Hert, Paul and Rocco Bellanova. 2011. *Transatlantic Cooperation on Travelers' Data Processing: From Sorting Countries to Sorting Individuals*. Washington, DC: Migration Policy Institute.

Table of Contents

Executive Summary

Efforts in the post-9/11 world to identify terrorists and serious transnational criminals have created new impetus for the collection and processing of increasing quantities of data. In particular, a vast array of data on international travelers is used for security purposes, ranging from basic identity and passport information to biometrics and personal data gathered from airlines' reservation and check-in systems, to sensitive information on health and criminal records. The use of the data and the systems designed to collect them are currently most developed in the United States, although the European Union (EU) is also introducing or has proposed similar systems and practices.

The appeal of data-intensive security screening takes various forms. Data can be collected in advance of travel, allowing scrutiny of individuals to occur at an earlier stage and allowing more time for screening. Collection of traveler data also allows governments to increase the intensity of the controls they exercise, making use of more detailed information about individuals, and reallocating resources towards those deemed to be most "risky." Governments once based the intensity of screening primarily on a traveler's nationality ("sorting countries"), but new sources of information allow them to focus more directly on personal characteristics ("sorting individuals"). Broadly, therefore, data processing is supposed to help border guards and immigration agencies maintain more effective control over cross-border movement, without hampering mobility.

However, data sharing and data processing raise a host of legal and political questions related to individuals' privacy and data-protection rights. They have created the need for transparent legal frameworks to regulate what governments do with the information and what rights they provide to the individuals whose data they use. This was the purpose of a series of agreements negotiated over the past few years between the European Union and the United States regarding Passenger Name Record (PNR) data and other kinds of information.

Information-sharing agreements are still in flux, however. The EU position on data protection has evolved and in the future the European Commission is expected to push for a more comprehensive data-protection framework. Meanwhile, the EU-US PNR agreement is also due to be renegotiated, and as more states develop the capacity and the inclination to process personal information for security purposes, new agreements will become necessary. Furthermore, discussions regarding the possible completion of a comprehensive transatlantic data-protection agreement are becoming more concrete, and the European Commission has already presented a draft mandate for negotiations.

Governments once based the intensity of screening primarily on a traveler's nationality ("sorting countries"), but new sources of information allow them to focus more directly on personal characteristics ("sorting individuals").

Several different issues arise from governments' use (and sometimes misuse) of travelers' data, and these are reflected to varying extents in data-sharing agreements. First, there is a concern that governments may justify the collection and processing of sensitive personal information as part of their efforts to combat terrorism and serious transnational crime, but subsequently *use* that data for broader and less urgent functions, such as for more minor crimes or even immigration-related offenses.

Second, the United States currently uses certain types of data, particularly PNR, not merely to seek information about specific individuals suspected of wrongdoing, but also to statistically analyze

passengers' characteristics or behavior to identify persons who *may* pose a security risk. Given that individuals identified through this process may face tangible consequences — for example, being wrongly denied travel or subjected to repeated screening — the use of statistical models in this way could violate the presumption of innocence, due process, and nondiscrimination. A third, related concern is that some of the information shared is inaccurate. Individuals may be harmed by these mistakes, but they are rarely compensated. Finally, a lack of transparency can make it difficult for individuals to understand how their data are used.

Negotiating information-sharing agreements in this complex legal and institutional terrain has not been easy. As the new negotiating period approaches for both a transatlantic data-protection agreement, and a separate PNR agreement, challenges lie ahead. As a result, some of the diplomatic tensions that surfaced in previous negotiations are likely to reemerge.

Differences between the United States and the European Union arise from several sources. Perhaps most important is that while both sides subscribe to similar basic principles when it comes to data protection and privacy, they have different legal and institutional structures and different approaches to implementing these principles, making common procedures and process difficult. Judicial redress and data minimization are areas of potential conflict, with some essentially procedural differences potentially paving the way for fundamental disagreements about actual policies.

Notwithstanding important differences and even bitter debates, the EU-US dialogue on data sharing has made significant progress. However, as the European Union and the United States enter the next phase of negotiations, the following recommendations will remain pertinent:

- Border-control policies should become more "friendly" to travelers and citizens, taking into account their legitimate interests. The right to compensation and judicial redress should also be central to efforts to guard against abuse, while helping to ensure that security controls are used to promote citizens' interests.
- Data processing and its consequences should be opened up to greater public scrutiny and debate. Regular assessments should be required to investigate privacy and data protection and the ways that relevant technologies are used. In this respect, the European Union can look to positive examples in the United States. Policymakers should also examine how these reporting exercises can facilitate effective political scrutiny of technologies.
- Technologies have a strong role to play in border control; however, technology is more than just a neutral instrument and its use often impacts on society in a more fundamental way. Hence, technologies deserve thorough attention and should not be adopted blindly.
- The use of statistical targeting exercises, their purpose, scope, and efficiency, as well as their potential consequences, remain unclear. The European Union should clarify its position on the use of profiling techniques, and policymakers on both sides of the Atlantic should acknowledge (and address) the political issues that their adoption raises.

I. Introduction

The most concrete form of transatlantic cooperation in the field of "human mobility"[1] is without doubt data sharing — the transfer of information about passengers to government authorities, and the series of agreements that govern this process. Cooperation on data-processing methods has evolved in response to government agencies' growing use of traveler data for security purposes. Governments now collect a vast array of data on passengers, ranging from basic identity and passport information, to biometrics and personal data gathered from airlines' reservation and check-in systems. Policymakers generally perceive these data as a central solution to a challenge they have faced over the past few decades: how to effectively screen and regulate increasing numbers of individuals moving across state boundaries in a rapid and cost-effective manner.

Travelers' data are supposed to help border guards and immigration agencies identify and prevent security risks, and allocate security resources in order to promote security without hampering mobility. The data also typically provide governments with *advance* notice of travelers' identity and characteristics. This makes the data an increasingly central pillar of governments' security strategies, which in recent years have often emphasized pushing the borders outwards: dealing with potential security threats and unwanted entries before they reach the border, and if possible before travelers who merit scrutiny leave from their point of departure.

However, data sharing and data processing raise a host of legal and policy questions related to individuals' privacy and data-protection rights.[2] Concerns about privacy, data protection, and the presumption of innocence (since data may be used to identify potentially risky individuals with no record of wrongdoing) have created the need for transparent legal frameworks to govern the collection, sharing, and use of passenger data. Over the past decade, therefore, the European Union and United States have negotiated and concluded a series of agreements on data sharing. The basic purpose of these agreements is to limit the potential negative consequences of data use for individuals, while providing legal clarity for airlines and other commercial carriers (as well as government bodies) who are asked to share passenger data.

Data-sharing agreements continue to evolve, as do the types of data they govern and the uses for which data are deployed. In recent years, EU-US negotiations on data sharing have been somewhat asymmetric, since for the most part the United States requested and used the data, while the European Union primarily sought assurances that its use would be limited to "legitimate" purposes considered less intrusive for passengers. However, policies based on the processing of personal data are also a central feature of EU justice and home affairs policymaking. Plans have been advanced to adopt EU-wide measures similar to the ones already implemented in the United States, with the February 2011 proposal for an EU Passenger Name Record (PNR) directive,[3] and will probably be discussed again in the future. That said, as data become more central to EU border security strategies, differences in

1 See Susan Ginsburg, *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders* (Washington, DC: Migration Policy Institute, 2010), 282-86.

2 Privacy and data protection are often considered the same right, particularly where data protection is seen as privacy for an era of the information society (data protection as a sort of "new privacy"). However, data protection is increasingly considered and framed as a different right, even if partially overlapping with privacy. Paul De Hert and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State," in *Profiling the European Citizen: Cross Disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth (Dordrecht: Springer, 2008), 275. For a presentation of the relevant laws in the European Union and United States on privacy and data protection applied to security measures, see Hiroyuki Tanaka, Rocco Bellanova, Susan Ginsburg, and Paul De Hert, *Transatlantic Information Sharing: At a Crossroads* (Washington, DC: Migration Policy Institute, 2010), www.migrationpolicy.org/pubs/infosharing-Jan2010.pdf; Paul De Hert and Rocco Bellanova, *Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?* (Brussels: European Parliament's Committee on Civil Liberties, Justice, and Home Affairs, 2008), www.ceps.eu/system/files/old/data-protectionEP.pdf; Hielke Hijmans and Alfonso Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?," *Common Market Law Review* 46 (2009), www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-06-02_Shortcomings_DP_EN.pdf.

3 European Commission (EC), "EU proposal for passenger data to fight serious crime and terrorism," (Press release, February 2, 2011), http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/120&format=HTML&aged=0&language=en&guiLanguage=en.

practice between the European Union and the United States will probably remain, not least because of a somewhat different approach to data protection in the European Union, but also due to different legal constraints and perceptions of needs.

This report explains EU-US data-sharing agreements and their implementation. It begins with an overview of the architecture of data collection and analysis on both sides of the Atlantic. It discusses the rationale for these policies, and the data-protection and privacy concerns they have provoked. It explains the numerous data-collection and processing initiatives in operation on both sides of the Atlantic, the bilateral agreements and unilateral policies that govern them, and considers some unresolved questions and areas of potential future conflict.

II. The EU and US Travelers' Data-Collection Architecture

Before explaining data processing and the data-protection questions raised with respect to passengers, we present an overview of the systems for collecting data on individuals traveling to and from the United States and the European Union. Various types of data sources exist, each containing different types of information used in different ways. Further, data may be collected in three different ways: some are collected directly from individuals by governments; some are collected from airlines by governments; and some information (typically law enforcement data) is passed directly between governments or government bodies. As will become clear later, some of these data-processing practices are governed by data-sharing agreements and others are not. In particular, data gathered directly from individuals tend not to come under the scope of data-sharing agreements.

A. Passenger Name Record Data

Passenger Name Record (PNR) is a term that denotes the commercial information provided by passengers on transatlantic journeys, collected by air or sea carriers and used for their ticketing, reservation, and check-in systems.[4] Given its commercial nature, PNR contain several kinds of information, ranging from names, addresses, passport numbers, and credit card information, to information on other passengers, travel agents, and even meal options. As one of the most detailed and personal data sources, it has gained enormous symbolic and practical significance in the debate about data sharing, and has been the subject of several international agreements, national measures, political and institutional clashes, as well as strong academic interest.[5]

4 EC, "Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries," *Official Journal of the European Union,* December 30, 2010.

5 Among recent academic works focusing on PNR systems and issues, see Evelien Brouwer, "The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?," *CEPS Working Document* (Brussels: Centre for European Policy Studies, 2009); Peter Hobbing, *Tracing Terrorists: The EU-Canada Agreement in PNR Matters* (Brussels: Centre for European Policy Studies, 2008), www.ceps.eu/book/tracing-terrorists-eu-canada-agreement-pnr-matters; Patryk Pawlak, *Made in the USA? The Influence of the US on the EU's Data Protection Regime* (Brussels: Centre for European Policy Studies, 2009), www.ceps.eu/book/made-usa-influence-us-eu%E2%80%99s-data-protection-regime; Els De Busser, "EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal?," *Utrecht Law Review* 6, no. 1 (2010), www.utrechtlawreview.org/index.php/ulr/article/viewFile/116/116; Vagelis Papakonstantinou and Paul De Hert, "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic," *Common Market Law Review* 46, no. 3 (2009). Many civil liberties watchdogs and advocates regularly publish reports and documentation related to PNR: Statewatch, "Observatory on the Exchange of Data on Passengers (PNR) with USA," Statewatch.org, www.statewatch.org/pnrobservatory.htm; Electronic Privacy Information Center (EPIC), "Air Travel Privacy," accessed December 13, 2010, http://epic.org/privacy/airtravel/; Privacy International, "Border and Travel Surveillance,"

www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Border+and+Travel+Surveillance&als[theme]=Border%20

In the United States, PNR data on all inbound passengers, including US citizens, are stored in a database where they are cross-referenced with other information, including other sources of passenger data and law enforcement data.[6] They are then used in various ways. First, data are used to identify known criminals or their associates. Second, PNR data are also analyzed in a statistical targeting exercise designed to identify persons who may pose a security risk, but who were previously unknown to Department of Homeland Security (DHS), the agency responsible for security and immigration issues in the United States.[7] For example, people sharing specific behavioral or travel patterns could be identified for secondary screening. Following this automated processing, officers at the National Targeting Center-Passenger (NTC-P) process the data of identified persons in order to carry out additional checks on their records.[8] Individuals are either confirmed as a potential security risk or are cleared. Additional manual checks are carried out to determine if suspected passengers are traveling with any similarly suspicious associates.[9]

Airlines are required to send PNR data to DHS up to 72 hours before departure. As a result, the processing of personal data and the eventual secondary screening can take place before passengers reach the United States or even before they have boarded at their point of departure. DHS can obtain and process information at a distance, in both spatial and temporal terms. This makes PNR data a component of the broader US border policy, which in recent years has increasingly sought to "push the border outwards," exercising some border-control functions before passengers reach the country.[10]

The European Union currently does not have an EU-wide PNR system, although in February 2011, the adoption of an EU PNR directive was proposed as part of the EU Stockholm Programme — the Council framework for policies to be developed in the area of Justice and Home Affairs in the period 2010-2014. The directive, which must be approved by the Council of Ministers and European Parliament, will replace a proposal presented by the Commission in 2007.

The PNR directive, proposing creation of an EU-wide PNR system not dissimilar to that used in the United States, has the goal of fighting "serious crime and terrorism."[11] Its goal would be to make PNR data available to "competent authorities" in EU Member States for the purpose of preventing and combating terrorism and organized crime.[12] A Passenger Information Unit (PIU) would be created in each Member State, and airlines would be required to send PNR data to that agency for every passenger entering or leaving the European Union.[13] These agencies would assess the risks passengers pose and would alert the relevant authorities about passengers requiring further investigation. Anonymized data would be used for risk assessments and analysis of travel trends for security purposes.[14] The PIU would be required to "immediately" delete any PNR data "revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life."[15]

and%20Travel%20Surveillance&conds[1][category.....]=Border%20and%20Travel%20Surveillance.

6 US Department of Homeland Security (DHS) Privacy Office, *2009 Data Mining Report to Congress* (Washington, DC: DHS, 2009), www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.

7 Ibid., 10.

8 Testimony of David V. Aguilar, Acting Deputy Commissioner, US Customs and Border Protection, before the Senate Homeland Security and Governmental Affairs Committee, *The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening*. 111th Cong., 2nd sess., March 10, 2010, 4-7, www.cbp.gov/linkhandler/cgov/newsroom/congressional_test/holiday_attack.ctt/holiday_attack.pdf.

9 EC, *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)* (Brussels: EC, 2010), 14.

10 Furthermore, as discussed in the latest PNR joint review of 2010, PNR data are also processed as part of US projects on immigration control run in several EU Member States, either *in loco* as in the case of the Immigration Advisory Program or remotely as in the case of the Regional Carrier Liaison Groups; Ibid., 15-16.

11 EC, "EU proposal for passenger data to fight serious crime and terrorism."

12 EC, "Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime" COM (2011) 32-11, www.eu-oplysningen.dk/euo_en/dkeu/status/status_en_20110032/?print=1.

13 Ibid., Article 1, 19.

14 Ibid., Article 9, 26.

15 Ibid., Article 11, 27.

The proposed directive promotes various types of data-protection safeguards. Indeed, during earlier internal Council negotiations regarding the 2007 proposal, a specific, ad hoc data-protection framework for the measure was drafted instead of the general EU data-protection framework for law enforcement that was initially foreseen. Nonetheless, the proposal was heavily criticized by some EU institutions and academics for not going far enough to protect individuals' data[16] or to guard against the risk of discrimination.[17]

B. *Advance Passenger Information*

Advance Passenger Information (API) is primarily biographical data found in passports with the addition of some information on the means and routes of transportation. Like PNR data, API is collected and used by air carriers (and other types of commercial carriers), but it is less extensive (PNR data usually include all of the information available as API). In both the United States and European Union, the development and implementation of API systems preceded the more extensive PNR systems.

In the United States, the use of API is designed to enhance national security by transmitting passenger information to US Customs and Border Protection (CBP) before visitors arrive on American soil.[18] The European Union has provisions for the use of API in Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data, widely known as the API Directive. This directive requires carriers to transmit advance passenger data to "competent national authorities" with the purpose of "improving border controls and combating illegal immigration."[19] Data are mainly used for "verification" purposes, and must be deleted after a limited retention period of 24 hours.[20] Note, however, that very few EU countries have implemented the API Directive. This is surprising given the pressure that the European Council exerted on the European Parliament in its emphasis on the relevance of API data to combating irregular migration and terrorism.[21] Furthermore, as is the case with the US API system, it is not clear how the API and PNR systems are expected to relate to one another.

From a data-protection point of view, when compared to other practices aiming at processing passenger data, the proposed EU API system differs from PNR in that less information is collected and data are held for a shorter period of time. As a result, the data can be used to verify identities but have much less potential to be used for assessing behavior or continuously feeding the "profiling machine."[22]

16 See Paul De Hert and Vagelis Papakonstantinou, "The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe," *Computer Law & Security Review* 26 (2010): 374-76; European Data Protection Supervison (EDPS), *Opinion on the Draft Proposal for a Council Framework Decision on the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes* (Brussels: EDPS, 2007).

17 See Brouwer, "The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom?," 20-24; European Union Agency for Fundamental Rights (FRA), "Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes," (Vienna: FRA, 2008), 10-13.

18 DHS, "Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels" Final Rule (Washington, DC: *Federal Register*, 2007), 48320.

19 EC, "Council Directive 2004/82/Ec of 29 April 2004 on the Obligation of Carriers to Communicate Passenger Data," Article 1, *Official Journal of the European Union,* 2004.

20 Ibid,. Article 6.

21 See Valsamis Mitsilegas, "Contrôle Des Étrangers, Des Passagers, Des Citoyens : Surveillance Et Antiterrorism," *Cultures & Conflits* 58 (2005).

22 In the words of the European Commission: "The uses of PNR data are very different from those of API data, largely due to the fact that a PNR contains very different types of data. PNR are mainly used as a criminal intelligence tool rather than as an identity verification tool. (…) PNR data are unique in their nature and their use. Such use can be: (…) pro-active (patterns): use for trend analysis and creation of fact-based travel and general behaviour patterns, which can then be used in real time use. In order to establish travel and behaviour patterns, trend analysts need to be allowed to use the data over a sufficiently long period of time. A commensurate period of retention of the data by law enforcement authorities is necessary in such cases." EC, "Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries," (Brussels: EC, 2010), 4.

C. *Data Collected Directly from Individuals*

In both the United States and the European Union, several programs exist to collect personal data directly from individuals. This process does not tend to be governed by data-sharing agreements. However, the programs are worth mentioning briefly because they form part of the overall data architecture.

1. Electronic Systems of Travel Authorization

In the United States, the Electronic System of Travel Authorization (ESTA) obliges citizens from Visa Waiver Program (VWP) countries[23] to send biographical data at least 72 hours prior to departure, allowing CBP to check them against several law enforcement databases. ESTA applications are valid for a maximum of two years or until the expiration of the foreign national's passport, and approval is required in order to board commercial transportation to the United States. This information is collected *in addition to* PNR and API data, and it includes the data generally collected in the document Form I-94W completed by citizens of VWP countries. Some of the data are the same as for PNR and API, but the form also contains sensitive information such as mental and physical health information and criminal records, as well as the destination address in the United States (data that can be linked directly or indirectly to third persons). ESTA data can be retained for up to 75 years.[24]

While the program began on a voluntary basis in August 2008, it became compulsory in January 2009; more recently a $14 fee has been introduced. The US government cites the cost of running the program as justification, but also earmarks a portion of the revenue for tourism promotion.

The European Union does not have an equivalent system, although a 2008 EU Commission Communication[25] proposed an electronic system of travel authorization requiring third-country nationals who are not required to hold visas to make an electronic application in advance of traveling, in which they would be asked to supply personal data, passport information, and travel details.[26] However, European reaction to the US implementation of the ESTA system has been mixed: despite declaring an interest in starting a similar program, the European Commission worried about the introduction of a new form of "disguised visa" and the more recent fee introduction reignited debate about unilateral US measures.

2. Registered-Traveler Programs

The idea behind registered-traveler programs is to allow individuals who are considered to present low risk — because they have provided key personal information and passed special screening — to pass through borders with only minimal (typically automated) screening. The United States operates registered-traveler schemes at its southern and northern land borders, as well as at airports; and some EU Member States such as the Netherlands and the United Kingdom have similar programs. While no EU-wide system has been developed so far, a 2008 European Commission proposal on border management strategy includes a registered-traveler system designed to accelerate processing at EU borders and ports of entry.[27] According to the proposal, the EU program would be available to both EU and non-EU citizens traveling back and forth to the European Union, and would essentially extend the

23 Travelers from 36 countries that have Visa Waiver Program (VWP) agreements with the US government are permitted to enter the country visa-free and remain for up to 90 days. See State Department, "Visa Waiver Program (VWP), accessed March 2, 2011, http://travel.state.gov/visa/temp/without/without_1990.html#vwp.

24 During the transition period and co-usage with a paper-based form, the data will be stored for the same period of validity of the ESTA approval, plus one year, plus another 12 years in archive, but still available for retrieval. After this 15-year period, the data will be archived under stricter rules of access.

25 EC, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the Next Steps in Border Management in the European Union," (Brussels: EC, 2008), 8.

26 Ibid., 9.

27 Ibid., 6.

use of "tailored" risk assessment in Europe.

3. Other Systems for Monitoring and Recording Entries (and Exits)

Various EU and US data systems are used in order to register entries. In the United States, the primary system of this kind is the United States Visitor and Immigrant Status Indicator Technology (US-VISIT), which collects biometrics (fingerprints and a digital photo) and certain biographical information from all foreign nationals (with exceptions for certain Mexican and Canadian nationals).[28] Launched in 2004, US-VISIT's original purpose was immigration management, although it has been recast to some extent as an antiterrorism tool since the September 11, 2001 terrorist attacks.[29] The information the program collects is checked against 20 interfacing government databases in order to determine if a visitor is listed as a criminal or a terrorist. Although Congress in 1996 mandated implementation of an entry-exit system, in hopes of identifying visa overstayers, US-VISIT does not have the capacity at present to record exits.

The European Union's Visa Information System (VIS), which is currently under development, will be a centralized EU database holding the personal information (including photos and fingerprints) of non-EU nationals who apply for a short-stay visa.[30] Its purpose is to combat visa fraud, facilitate checks at border crossings, and prevent security breaches.[31] VIS is another example of how migration management tools can be remodeled to become instruments of national security, and in this respect it is similar to the US-VISIT system. The two systems differ, however, in their relationships with other databases and data-processing systems. While US-VISIT information is matched against several other systems, the VIS database remains isolated from other systems and law enforcement agencies can only access the data on specific cases and under restricted conditions.[32]

In addition, the EU Stockholm Programme envisages the development of an entry-exit system, designed to identify visa overstayers, which would register arrivals and departures by third-country nationals, whether or not they were required to hold visas.[33]

III. Using Data for Screening Passengers: Sorting Countries and Sorting Individuals

Why do governments turn to personal data when screening travelers? Traveler information is used for two purposes. First, the data can be used for formal security reasons, where the primary purpose is police cooperation, counterterrorism, or tackling organized international crime. Second, some data are kept more directly for the purposes of managing the immigration system: for example, recording entries or processing visa and asylum requests.

28 Electronic Privacy Information Center (EPIC), *Privacy and Human Rights, an International Survey of Privacy Laws and Developments* (Washington, DC: EPIC and Privacy International, 2006), 12.
29 Peter Hobbing, *A Comparison of the Now Agreed Vis Package and the US-Visit System* (Brussels: European Parliament, Policy Department C - Citizens Rights and Constitutional Affairs, 2007), 5.
30 EC, "Regulation (Ec) No 767/2008 of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (Vis) and the Exchange of Data between Member States on Short-Stay Visas (Vis Regulation)," *Official Journal of the European Union*, 2008.
31 Ibid., Article 3.
32 Article 5, "Council Decision 2008/633/Jha of 23 June 2008 Concerning Access for Consultation of the Visa Information System (Vis) by Designated Authorities of Member States and by Europol for the Purposes of the Prevention, Detection and Investigation of Terrorist Offences and of Other Serious Criminal Offences," *Official Journal of the European Union*, 2008.
33 Council of the European Union, The Stockholm Programme - an Open and Secure Europe Serving and Protecting Citizens," 95.

However, there are cases of overlap between the two purposes. On the one hand, many of the systems created for migration purposes have integrated security functions into their purview, mainly by allowing law enforcement agencies to access them under certain conditions, or by running the data collected and stored against other databases. On the other hand, some sets of travelers' data and some channels of data exchange can also be used in migration management tasks. In a 2010 report, for example, the European Commission expressed concerns that PNR data, whose purpose is supposed to be limited to combating terrorism and serious transnational crime, seems to be used in efforts to prevent illegal immigration by matching PNR to ESTA data and prior visa refusals.[34] Also, some data-sharing channels can be "activated" for some forms of migration management where migration-related actions are listed as criminal offenses.[35]

A. The "Dream of Targeted Governance"

The collection and processing of personal data for security and immigration purposes are part of a new, more technological approach to screening travelers entering or seeking to enter a country's territory. Traditionally, policymakers determined the level of screening that an individual would require primarily on the basis of nationality. That is, nationals of certain countries were required to obtain a visa (and hence undergo scrutiny at a consulate), while others could enter with just their passport.[36] This approach remains in place today in the form of the VWP and similar exemptions provided by the European Union, and relies on "sorting countries" rather than "sorting individuals."[37]

However, with the greater ability to store and process data electronically, governments have been able to move closer to the idea of sorting individuals: focusing on an individual's characteristics, not just their nationality. Of course, the traditional country-based approach is not likely to disappear, but instead is integrated with this new focus on individuals. Note that sorting individuals implies a "redistribution" of screened people into different categories or groups, such as bona fide travelers or risky travelers. In practical terms, it can mean different levels of control performed at different stages of the journey: some individuals who would face lower levels of screening on the basis of their nationality might now face more extensive controls, while others (particularly registered travelers) face lower levels of screening — at least at the port of entry. Of course, PNR data in particular are also collected not just for foreign nationals but for citizens who are also "risk assessed" and vetted in advance.

In other words, data processing of the kind described in this report allows a more sophisticated approach towards risk, reducing the need for a "one-size-fits-all" approach while at the same time extending the range of possible controls. The most commonly stated goal of these new forms of data processing is to improve migration management by allowing resources to be reallocated from less risky individuals to more risky ones. This approach is also evident in the increasingly promoted registered-traveler programs. In fact, these trusted-traveler programs can offer an apparently politics-free solution to a delicate foreign policy issue, since they allow governments to maintain broad screening controls while smoothing the entrance of "selected" people[38] who are not considered to pose a threat. However,

34 EC, *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)* (Brussels: EC, 2010), 11 & 15-16.

35 Providing a comparative study of which countries "criminalize" migrants, and how they do this is beyond the scope of this paper. However, the authors believe this exercise to be increasingly necessary to understand the proportionality and effective use of the measures presented in this section.

36 For the EU list, see *Official Journal of the European Union*, "Regulation (Ec) No 539/2001 Listing the Third Countries Whose Nationals Must Be in Possession of Visas When Crossing the External Borders of Member States and Those Whose Nationals Are Exempt from That Requirement," 2001. For an overview of US visa-free travel initiatives, see Ginsburg, *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders*, 282-86.

37 The concept of "sorting individuals" is partially drawn from the reflections of David Lyon, "Surveillance as Social Sorting: Computer Codes and Mobile Bodies," in *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, ed. David Lyon (London: Routledge, 2003).

38 See Ginsburg, *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders*, 277-308.

questions remain regarding the effectiveness of such programs, especially when they are mainly promoted as a solution to security concerns, since they may still be vulnerable to security breaches.

Much of the appeal of data processing for controlling human mobility, therefore, derives from the idea of greater efficiency in allocating resources. As such, it can be considered part of a broader modern phenomenon: what has been called the "dream of targeted governance," or the desire to concentrate the resources of the state and its agencies on specific issues and individuals.[39] Policymakers in fields ranging well beyond immigration and national security have sought to use data — as well as the rapid processing and extensive storage capacity that are now technologically possible — in order to identify targets of action that should receive priority, and to understand those targets better.

B. *Passenger Data and the Evolution of Border Security Strategies*

A second reason for governments' use of travelers' data — and particularly commercial PNR data — is that it enables new *types* of screening due to the very nature of the information involved. Individuals create an enormous quantity of nonadministrative data in the course of their daily lives, most of which is "dispersed" and is never captured and processed in one place. PNR initiatives represent an attempt to capture at least some of this nonadministrative, biographical data in order to understand individuals' characteristics and behavior. Concerns about this type of data collection, of course, abound (evident, for example, in the appearance of phrases such as "biometric state"[40] or "database state"[41]). We will discuss these concerns shortly.

Finally, data transfers of the kind described here have also allowed governments to extend their scrutiny of human mobility to a much earlier stage in the process. Rather than waiting for travelers to arrive on their territory, security and immigration agencies, using a wide range of programs, can monitor travel from its very first step — booking a ticket — or receive and store information about travelers even further in advance through registered-traveler schemes. This has been one of the most significant phenomena of modern border management, particularly in the United States, and remains so notwithstanding the change of occupants in the White House. In May 2010, the White House released the latest US National Security Strategy, the first since President Obama took office.[42] This document affirms the administration's desire to "bolster aviation security worldwide through a focus on information collection and sharing, stronger passenger vetting and screening measures, the development [...] of advanced screening technologies, and cooperation with the international community to strengthen aviation security standards and efforts around the world."[43]

39 Mariana Valverde and Michael S. Mopas, "Insecurity and the Dream of Targeted Governance," in *Global Governmentality,* eds. Wendy Larner and William Walters (New York: Routledge, 2004).

40 Benjamin J. Muller, *Security, Risk and the Biometric State: Governing Borders and Bodies*, eds. Peter J. Burgess and Prio New Security Studies (London/New York: Routledge, 2010).

41 Ross Anderson, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, and Angela Sasse, *Database State* (York, UK: The Joseph Rowntree Reform Trust Ltd., 2009), www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf.

42 White House, "National Security Strategy," (Washington, DC: White House, 2010), www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

43 Ibid., 20.

IV. Data Protection, Privacy, and Other Concerns about the Use of Personal Passenger Data

The use of data and technology may be a constant in modern public policy, but it raises some difficult issues.[44] In particular, governments continue to grapple with the appropriate level of data protection and privacy, and with the consequences and impacts of relying on large-scale databases containing personal information. Recent judgments by European courts have also challenged the proportionality and necessity of certain government uses of data for security purposes, as we briefly discuss.

One of the main issues is the "transparency" of the data processing itself. In a recent case, *Liberty & Others vs. United Kingdom,*[45] the European Court of Human Rights (ECHR) determined that the UK government's use of telecommunications interception data was not "in accordance with the law" because it did not provide adequate safeguards against the abuse of power and gave the state excessive discretion to intercept communications. Even more interestingly, the ECHR judgment also criticized a lack of transparent procedures for storing, analyzing, and retaining data, and emphasized that governments must "unveil" their data-processing practices while enabling the public to understand the "sorting process." In other words, the judgment recognizes that data processing is not simply a technocratic task, but can have a tangible impact on individuals. These issues certainly arise in the case of PNR data use, where the ways in which data are processed are still far from clear.[46]

A second case before the same court[47] examined the retention of data (in this case, of DNA and biometrics). The ECHR judgment ruled that retaining and storing data on individuals can have a direct impact on their "private life interest" even if the data are not subsequently used;[48] and that as a result, data should be retained for strictly limited periods.[49] In other words, the "mere retention" of data is not a trivial activity, and surveillance at a distance has consequences for both individuals and societies.[50] This judgment is particularly relevant to information-sharing agreements because they permit transmission of data for large numbers of individuals who are not guilty (indeed, who are not even suspects in the traditional sense); and because in many cases the retention periods are long. Where PNR data are used to build risk profiles and model patterns of traveler behavior, long retention periods (up to 15 years in the most recent US-EU PNR agreement) have created particular concerns.[51]

A third problem is that in some cases, the use of traveler data for security purposes may violate the presumption of innocence or create barriers to mobility. Risk-assessment exercises, as we discuss shortly, could lead to errors with real consequences for individuals, such as being denied boarding or being repeatedly subject to extra screening measures. The matching of personal data against inaccurate

44 Note that a large body of research discusses data-protection laws in some detail. See, for example, De Hert and Bellanova, *Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?*; Tanaka et al., *Transatlantic Information Sharing: At a Crossroads;* Maria Veronica Pérez Asinari and Pablo Palazzi, eds., *Défis Du Droit À La Protection De La Vie Privée-Challenges of Privacy and Data Protection Law* (Brussels: Bruylant, 2008); Francesca Bignami, "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," *Boston College Law Review* 48 (2007).

45 *Liberty & Others V. The United Kingdom*, (2008).

46 Two of the most common reasons justifying the "opacity" of processing techniques from governments' perspective are the fear of exposing systems to a higher rate of "countermeasures;" and specific types of data and analysis becoming more or less important over time, on the basis of intelligence updates. State agencies often invoke the second reason as a motivation for retaining data as long as possible since the information "may" become important in the future.

47 *S. And Marper V. The United Kingdom,*(2008).

48 Section 121, Ibid.

49 Section 125, Ibid.

50 In a certain way, this judgment is close to the reasoning of the Romanian Constitutional Court on the national implementation of the data-retention directive.

51 Regarding arguments for the need for long data-retention periods, see EC, "Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries;" EC, "Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes."

information or inaccurate watch lists can also lead to serious consequences for individuals.[52] The impact of data-related policies on travelers, including their economic and commercial interests, has gained little consideration, however. When errors or inevitable inaccuracies in data processing lead to false alerts, individuals are very rarely compensated financially for the harm they suffer.[53]

Finally, there is a more general concern about whether the collection, use, and retention of personal data are proportionate to their goal, and whether data will become subject to "mission creep." In most cases, data-collection policies were developed with the purpose of preventing terrorism and serious crime, in the interests of EU and US citizens. If the eventual use of the data becomes much broader (for example, if it is collected for the purposes of counterterrorism but is used for the purposes of preventing illegal immigration) it could be argued that the potential damage to individuals is no longer proportionate to the policy's goal. A recent judgment by the European Court of Justice (ECJ) on the potential reestablishment of border controls within the Schengen zone (even when "disguised" as police controls) confirms this stance, stating that transnational cooperation should ultimately benefit individuals, among other things to relieve them from the burden of excessive controls.[54]

Profiling and Data Mining

Profiling and data mining are worth describing in more detail because they are the activities that raise most questions. They also have attracted increasing attention during the last few years. Profiling activities fall into two categories. On the one hand, profiling can mean using data to build up a picture of a certain individual where there is reasonable suspicion that the individual poses a threat. On the other hand, pattern-based searches — generally known as data mining — can be used to *detect* individuals who might pose a threat, even when no specific individual presents a known or suspected risk. This second approach relies on the power of the statistical model that is used to identify suspicious individuals. As a result, the approach has been criticized for its potential to intrude in known and unknown ways into the lives of innocent people whose characteristics appear (statistically) to be suspicious.[55]

These concerns are not new, nor are the practices that create them. But regulating the use of data mining in data-sharing agreements is complicated by the fact that no common EU-US definition exists, and no EU definition exists at all. The United States has adopted a legal definition of data mining and requires a certain level of transparency for government bodies that deploy it. Data mining in the United States is defined as "a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where — (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals."[56] The legislation that contains this definition requires department or agency heads to report to Congress if they use data-mining techniques and outline the ways in which they intend to analyze the data.[57]

52 One example in which inaccurate information had very serious consequences is the case of Maher Arar, a Syrian-born Canadian citizen who was detained during a stopover in the United States on possible suspicion of terrorist ties and deported to Syria where he is widely believed to have been tortured. An enquiry into the Arar case was held in Canada. See Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar* (Ottawa: Gilmore Print Group, 2006).

53 To our knowledge, no security-related legislation specifically implies the possibility for financial compensation.

54 European Court of Justice, *CJ, June 22, 2010, judgment, C-188/10 and C-189/10, Aziz Melki and Selim Abdeli, judgment of June 22, 2010, C-188/10 & C-189/10*, http://ec.europa.eu/dgs/legal_service/arrets/10c188_en.pdf.

55 Ira S. Rubinstein, Ronald D. Lee, and Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches," *The University of Chicago Law Review* 75, no. 1 (2008): 263.

56 *The Federal Agency Data Mining Reporting Act*, Pub. L. 110-53, 121 Stat. 266 Section 804(b)(1).

57 Ibid.

In contrast, EU legislation lacks a specific definition of profiling and data mining.[58] EU documents and European Commission proposals generally prefer to define activities of this kind as "risk assessment." For example, the European Commission communication on the global approach to PNR transfer describes the PNR risk-assessment uses in terms such as "re-active," "pro-active," and "real-time," which all imply the processing of data either in search of correlation or detection.[59]

V. Policies and Agreements on Transatlantic Data Sharing

As governments began to seek more data and use the information for more purposes over the past decade, concerns about potential negative consequences for individuals grew. In order to address some of these concerns,[60] particularly those arising from the use of the detailed, commercial PNR data, the European Union and United States have developed a series of principles and common practices. While some of these principles have been enshrined in previous agreements as part of ad hoc data-protection guarantees, they remain a work in progress and continue to be negotiated and renegotiated, as we explain shortly.

Three of the eight agreements in place between the European Union and the United States in the field of security and mobility concern some form of information sharing:[61] the PNR agreement, the Mutual Legal Assistance Agreement, and the EUROPOL-US Agreement. These agreements allow for the exchange of personal data collected from individuals traveling between the United States and EU Member States. Note, however, that they involve substantially different types of information. The PNR agreement governs the use of "raw" data gathered from commercial carriers and states the uses for which it can be put; this agreement is the main focus of our analysis, since it raises some of the most difficult legal questions and will be the subject of significant further negotiations. Next to the ongoing PNR agreement negotiations, a second track will start in the meantime, with the goal of establishing a more comprehensive transatlantic data-protection framework, covering police and judicial cooperation. We present both the background work done by the High Level Contact Group of EU and US experts, as well as the European Commission mandate that has been adopted by the Council as the negotiating basis. Finally, we also briefly discuss two other agreements which involve the sharing of data *between government bodies* on specific criminal or terrorist suspects.

A. The Passenger Name Record Agreement

Few security measures have attracted as much attention as the processing of PNR, and few have generated such tension among public, private, and individual actors.[62] PNR has attracted growing

58 Apparently, at the EU level, only the European Parliament seems particularly keen on formulating a legal definition of profiling: see European Parliament, *Report with a Proposal for a European Parliament Recommendation to the Council on the Problem of Profiling, Notably on the Basis of Ethnicity and Race, in Counter-Terrorism, Law Enforcement, Immigration, Customs and Border Control* (Brussels: Committee on Civil Liberties, Justice, and Home Affairs, 2009).

59 EC, "Communication from the Commission. On the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries," 4.

60 For a more detailed presentation of EU-related systems, see the 2010 Communication of the European Commission, "Communication from the Commission to the European Parliament and the Council. Overview of Information Management in the Area of Freedom, Security and Justice," (Brussels: European Commission, 2010). For a quick overview of the main axes of EU-US cooperation against terrorism, see Kristin Archick, *U.S.-EU Cooperation against Terrorism* (Washington, DC: Congressional Research Service, 2010), www.fas.org/sgp/crs/row/RS22030.pdf.

61 The eight agreements are: the Terrorist Financing Tracking Program agreement; the 2007 Passenger Name Record agreement; the two US-EUROPOL agreements (one strategic and one operational); the US-EUROJUST agreement; the EU-US Mutual Legal Assistance Agreement; the EU-US Mutual Extradition Agreement; and the Container Security Initiative.

62 Only the so-called SWIFT agreement, or Terrorist Financing Tracking Program, has generated a similar amount of attention and tensions.

public attention since the adoption of the *US Aviation and Transportation Security Act* in November 2001. The law required that CBP access passenger data for all US-bound flights. As a result, passenger information now officially plays a larger role in law enforcement measures to combat terrorism and international crime. However, there are relatively few publicly available assessments of the effectiveness of PNR processing, and it is not clear to what extent the data have been successfully used in counterterrorism efforts.[63] Public reports also do not specify to what extent positive outcomes are reached by the "simple" matching of data as opposed to by data mining, or if all of the data presently collected prove useful in the exercise of law enforcement.

The original rationale for an agreement on PNR sharing arose from the data's commercial nature. European airlines were reluctant to hand over personal data to the US authorities for fear of violating EU laws on data protection and privacy. In other words, the PNR agreement began as a kind of "safe harbor" provision for commercial entities transmitting data to the US government for security purposes, so that they would not be liable for breaking EU laws.

The first agreement, signed in 2004 was terminated by an ECJ ruling in 2006 in a case brought against the European Commission by the European Parliament. The ECJ ruling determined that the European Commission made the decision to approve the agreement without an appropriate legal basis. A second (interim) agreement signed in 2006 expired a few months later in 2007.[64] The most recent EU-US PNR agreement,[65] reached in 2007, is the third agreement to have been signed. However, this 2007 agreement is also in the process of renegotiation, because its ratification by the 27 Member States was not completed before the entry into force of the Lisbon Treaty. Hence, new rules apply, and the European Parliament's consent is required in order to conclude the agreement formally.[66] (The European Parliament has often expressed concerns and criticisms about the privacy and data-protection safeguards outlined in previous agreements.)[67] The EU Commission and the Council of the European Union have also finally agreed to start the negotiations of all three EU PNR agreements (with the United States, Canada, and Australia) at the same time, in order to ensure a certain level of consistency.[68] Pending ratification, the latest agreements are still applied on a provisional basis.[69]

The current US-EU PNR agreement is composed of a set of three documents. The first is the agreement itself, which provides a legal basis for the transmission of PNR data by transportation operators to the US Department of Homeland Security (DHS). The other two documents are "letters" exchanged between

63 See in particular, EC, "Communication from the Commission to the European Parliament and the Council. Overview of Information Management in the Area of Freedom, Security and Justice," 41.

64 See *European Parliament V Council of the European Union (Case C-317/04) and Commission of the European Communities (Case C-318/04). Joined Cases C-317/04 and C-318/04,*(2006). For a critical overview of the PNR agreements' saga, see Papakonstantinou and De Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic.*

65 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* L204/17, 4.8.2007.

66 The other two PNR agreements signed by the European Union will also be renegotiated: the EU-Canada agreement because it has expired, and the EU-Australia agreement for the same reasons as the EU-US one. In October 2010, "the three mandates should be identical in content and adopted at the same time; (…) [and] once the mandates are adopted, negotiations with the three partner countries should start simultaneously," Council of the European Union (Press release, 3034th Council Meeting Justice and Home Affairs. Luxembourg, October 7-8, 2010), 11.

67 The European Parliament's interest in the negotiations of the next PNR agreement remains very high, with strong support for enhanced data-protection and privacy guarantees; see two adopted resolutions, European Parliament, "European Parliament Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) Agreements with the United States, Australia and Canada," (Brussels: European Parliament, 2010); European Parliament, "European Parliament Resolution of 11 November 2010 on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries, and on the Recommendations from the Commission to the Council to Authorise the Opening of Negotiations between the European Union and Australia, Canada and the United State," (Brussels: European Parliament, 2010).

68 Council of the European Union, "Press Release. 3051st Council Meeting. Justice and Home Affairs. Brussels 2-3 December 2010," 7.

69 For a critical assessment of the evolution of the EU-US PNR agreements, see Vagelis Papakonstantinou and Paul De Hert, "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic," *Common Market Law Review* 46, no. 3 (2009).

the United States and the European Union. The US letter to the European Union is the core of the entire PNR agreement. There, it is stated that DHS will only use EU data for the purposes of combating serious transnational crime and terrorism or in order to protect the interests of the "data subject" (the individual about whom the data are collected) during judicial proceedings.[70] The letter lists the types of information that can be collected and procedures for handling sensitive data. Finally, it sets the period of data retention: seven years in an analytical database followed by eight years in a "dormant, non-operational status."[71] The EU letter to the United States acknowledges the assurances offered in the US letter, presenting them as providing the necessary basis for an adequate level of data protection.[72]

B. *Recent Developments in the Evolution of the Transatlantic Data-Protection Framework*

In the coming years, the framework for transatlantic data protection and data processing will continue to evolve. Indeed, since the 2007 PNR agreement was signed, significant developments in EU-US negotiations on data protection have taken place. Moreover, further changes in the architecture of EU data protection for law enforcement exchange and processing of personal data remain likely, both to keep pace with the changes implied and required by the Lisbon Treaty and to provide for a more coherent data-protection framework.[73] Finally, the recent adoption of the European Commission mandate for the negotiations of a comprehensive transatlantic data-protection agreement will probably imply further debates and changes.

Contrary to other authors,[74] and as we have discussed in previous work, we do not believe that EU and US divergences result simply from different philosophical conceptions such as liberty or dignity. Instead, we think that both sides have similar principles but that they implement them in different ways and through different legal and institutional structures.[75] For example, both sides agree that the purposes of data processing should be limited, but the United States envisages somewhat more extensive use. EU and US policymakers both foresee a role for oversight authorities, but EU law requires that these authorities retain a high level of political independence, while US authorities are more likely to be "embedded" within the executive branch. Different approaches to implementing judicial redress have also created tensions, as discussed shortly. Disagreements, it must be noted, are not necessarily easy to resolve simply because they are procedural in nature. A given process for data protection or privacy on one side of the Atlantic, for example, cannot necessarily be directly "applied" on the other. At the same time, different approaches to implementing common principles (for example on profiling) can result in divergent security policies, thereby failing to resolve conflicts. As a result, the main challenge is to find a solution that enables a high common standard rather than resorting to the lowest common denominator.

The High Level Contact Group (HLCG)

In order to tackle continuing concerns and disagreements about data protection and privacy, the European Union and United States established a High Level Contact Group (HLCG) in November 2006. The group was composed of senior officials from DHS and the Department of State, and from the

70 Section I of the US letter to the European Union.

71 Section VII of the US letter to the European Union. While dormant, data can be still accessed under stricter rules and on specific cases.

72 De Busser critically points out that "the EU did not comply with its own data protection standards when agreeing to an exchange of personal data with an administrative authority which can share the data with other authorities in the US for the purposes of criminal investigations. (…) the data protection safeguards which the EU requested are not vey apt to remedy this situation," De Busser, "EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal?," 100.

73 See Hijmans and Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?"

74 James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *Public Law & Legal Theory Research Paper Series*, no. 64 (2004).

75 De Hert and Bellanova, "Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?"

European Commission, Council of the European Union, and the EU Presidency. Its final report, published in 2008,[76] identified a series of common principles and concerns[77] and proposed two policy options: a soft law instrument (or nonbinding agreement) and a binding agreement providing further guarantees and safeguards. The final report stated a preference for a binding agreement, and after positive political feedback in favor of this option in Europe, the EU Commission has taken the same position.

The HLCG represents an advance in the EU-US conversation, because it suggests that agreement is possible on a wide range of key issues, such as purpose limitation, proportionality, sensitive data, and even redress and independent oversight. However, the HLCG was not able to smooth out all of the EU-US differences and it proved relatively difficult to establish common language and reconcile conflicting interpretations on some of the most sensitive issues. For example, the HLCG dismissed as minor differences in the definition of law enforcement on both sides of the Atlantic, but these differences are crucial because they risk opening the way to "mission creep." In addition, the contact group was not able to reconcile differences concerning judicial redress. The European Union experts argued that EU citizens should, if necessary, have access to US courts for judicial redress through the *US Privacy Act* if their data are misused; but US law limits these rights to US citizens and legal permanent residents.[78] By contrast, the European Union envisages that travelers will have access to judicial redress in EU courts regardless of their nationality.

In order to resolve certain conflicting interpretations of common principles, and especially those that would require a change in US statutes and laws, a binding international treaty — not the more commonly used executive agreement — would be required. This would not change the procedure at the EU level, but the adoption of an international treaty would require ratification by the US Senate, making agreement more difficult.

C. Commission Mandate for the EU-US Data-Protection Agreement

In May 2010, the EU Commission presented a draft mandate for future negotiations with the United States on data protection, following public consultation in the first months of 2010.[79] Since the draft mandate was confirmed in the European Council at the beginning of December 2010, this text would represent the EU position during future negotiations.[80] The mandate envisages significantly stricter data-protection rules than are currently in place.[81]

76 Council of the European Union, *EU US Summit, 12 June 2008. Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection* (Brussels: Council of the European Union, 2008), 3.

77 The list of common principles includes: (i) Purpose Specification/Purpose Limitation; (ii) Integrity/Data Quality; (iii) Relevant and Necessary/Proportionality; (iv) Information Security; (v) Special Categories of Personal Information (sensitive data); (vi) Accountability; (vii) Independent and Effective Oversight; (viii) Individual Access and Rectification; (ix) Transparency and Notice; (x) Redress; (xi) Automated Individual Decisions; (xii) Restrictions on Onward Transfers to Third Countries. The pending questions were: (i) Consistency in private entities' obligations during data transfers; (ii) Equivalent and reciprocal application of privacy and personal data-protection law; (iii) Preventing undue impact on relations with third countries; (iv) Specific agreements regulating information exchanges and privacy and personal data protection; and (v) Issues related to the institutional framework of the European Union and the United States, Ibid. For a critical overview of the works of the HLCG, and in general on EU-US negotiations in privacy and data protection matters, see Tanaka et al., *Transatlantic Information Sharing: At a Crossroads*, 34-38.

78 Council of the European Union, *EU US Summit, 12 June 2008. Final Report by EU-US High Level Contact Group*.

79 EC, "Proposition De Recommandation Du Conseil Autorisant L'ouverture De Negociations En Vue D'un Accord Entre L'union Européenne Et Les États-Unis D'amérique Sur La Protection Des Données Personnelles Lors De Leur Transfert Et De Leur Traitement À Des Fins De Prevention, D'investigation, De Detection Ou De Poursuite D'actes Criminels Y Compris Le Terrorisme, Dans Le Cadre De La Cooperation Policiaire Et Judiciaire En Matiere Penale," (Brussels: EC, 2010).

80 Council of the European Union, "Press Release. 3051st Council Meeting. Justice and Home Affairs. Brussels 2-3 December 2010," 27. The Council press release does not specify if the mandate was amended or not, but the key elements of the text of the mandate are briefly reprised. For this reason, and until the release of the official version, we assume that the text has not been substantially modified.

81 EC, Section 1 of the Negotiating Directives, "Proposition De Recommandation Du Conseil Autorisant L'ouverture De Negociations En Vue D'un Accord Entre L'union Européenne Et Les États-Unis D'amérique Sur La Protection Des Données Personnelles Lors De Leur Transfert Et De Leur Traitement À Des Fins De Prevention, D'investigation, De Detection Ou De Poursuite

According to the latest version made public, it confirms that the scope of data transfers should be limited to the "purpose of preventing, investigating, detecting or prosecuting crime, including terrorism."[82] In addition to these basic principles, the draft mandate contains some very interesting and partially innovative provisions.

First, it would not only apply to all future agreements on data sharing involving the European Union or its Member States for the purposes of combating terrorism and serious crime;[83] but all previous agreements would also need to be brought into conformity with the new guidelines within three years. This includes transatlantic agreements such as PNR, and also agreements concluded between the United States and individual EU Member States. It could have some relevance for data transfers between government bodies of the kind discussed shortly, although its impact in this field would be more limited.

In other words, while the European Commission acknowledged the relevance of the HLCG work, it went beyond the HLCG position to strengthen data-protection measures further — and hence implies some likely tensions and disagreements in future negotiations.[84] For example, it proposed protection for all data subjects without discrimination on grounds of nationality — in other words, both EU and non-EU citizens would receive the same protections. Second, it introduces the principle of data minimization — the collection of the minimum amount of data required, and the progressive erasure of data unrelated to processing purposes — and the establishment of appropriate time limits for deletion. Third, it establishes the obligation of communicating security breaches. And finally, it envisages rights of both administrative and judicial redress, and even the right to compensation.[85] In this sense, the draft mandate not only takes a strong stance in relation to pending questions highlighted by the HLCG, but even adds further safeguards.

That said, the European Commission does envisage one significant exemption. Data-protection provisions would not apply to criminal intelligence when a national security interest was at stake.[86] The definition of national security would, according to the European Commission, be "narrow"[87] although the lack of specificity (and the fact that the European Union does not have an official definition of national security)[88] could lead to conflicting EU and US interpretations. This is especially the case since "national security" in the United States can encompass a very wide range of activities, including many of the essentially immigration-related functions for which traveler data are used. In other words, the effect of this exclusionary clause is far from clear.

D. *Transfers of Data between EU and US Government Bodies or Authorities*

The transfer of data between governments or official bodies is also worth a brief mention. These transfers differ in that they require direct and explicit coordination between governments — unlike data collection

D'actes Criminels Y Compris Le Terrorisme, Dans Le Cadre De La Cooperation Policiaire Et Judiciaire En Matiere Penale," as well as considering core elements for data-protection agreements with third countries for law enforcement purposes, which may include, where necessary, privately held data.

82 Ibid.

83 Ibid., Section 6 of the Negotiating Directives.

84 Some of the potential tensions in future negotiations were advanced by US Ambassador to the European Union William E. Kennard during a European Parliament hearing on October 25, 2010; see Edward Cody, "Armed with New Treaty, Europe Amplifies Objections to U.S. Data-Sharing Demands," *The Washington Post*, October 26, 2010.

85 EC, Section 7 of the Negotiating Directives.

86 Ibid, Section 11 of the Negotiating Directives.

87 Ibid.

88 The term "national security" is mentioned only one time in the full text of the Treaty on the Functioning of the European Union (TFEU) (*Official Journal of the European Union,* May 9, 2008, C 115, 49-199), in Article 73, in reference to cooperation between Member States' departments, but outside the framework of police and judicial cooperation (thus, *de facto*, refers to secret services). It also appears in the Schengen Convention, but also there it refers to Member States' internal security, and not to a possible EU-wide form of security. Recently, the first EU Internal Security Strategy was adopted, but again the concept of national security has not been used, and the scope of the entire strategy is particularly wide and covers most of the measures relying on data processing; see *Council of the European Union, Draft Internal Security Strategy for the European Union: "Towards a European Security Model"* (Brussels: Council of the European Union, 2010).

from commercial companies which can, in theory, be done unilaterally, although in practice requires a set of legal guidelines. Various EU-US agreements provide for data transfers of this kind for combating serious crime and terrorism. In general, these agreements have been less controversial because they generally do not govern the use of "bulk" data (which can be mined) but instead are used to answer direct queries about specific suspicious individuals.

The Mutual Legal Assistance (MLA) agreement between the European Union and the United States finally entered into force in 2010. It provides for collaboration on law enforcement issues. The agreement does not explicitly call for the sharing of data for migration management purposes, but it does provide for the exchange of personal data in order to further criminal investigations or prosecutions.[89] The MLA provides for symmetrical reciprocity in the transmission of personal data, contrary to the design of the PNR agreement which has so far largely consisted of a one-way flow of information from the European Union to the United States.

Another agreement, between the United States and EUROPOL, was signed in 2002 with the purpose of preventing crime in both jurisdictions. This agreement extends EUROPOL-US cooperation to the exchange of information, including personal data.[90]

Finally, a set of bilateral agreements between the United States and various EU Member States exists to allow the exchange of DNA and other biometric data for the purposes of enhancing cooperation in preventing and combating serious crime, namely terrorism.[91] The first agreement was signed with Germany, and several others have followed.[92] One controversial aspect of some of these agreements is that they were concluded as a *quid pro quo* for the accession of various Eastern European Member States into the US Visa Waiver Program allowing visa-free travel to the United States.

The data exchange in these agreements is based on the principle of a hit/no-hit system. Under this system, information is first checked against existing databases; only if there is a "hit" can comprehensive data be exchanged. As a result, the opportunities for data mining and processing are relatively limited. However, governments can supply more detailed personal data if they choose to do so. The information transmitted can potentially include sensitive data such as health information, sexual orientation, or trade union membership if it is considered relevant to an investigation. These agreements contain a specific framework for data protection; however, these rules would likely have to be brought into conformity with any new EU framework for data protection implemented in the future.

E. Data-Sharing and Processing Practices Involving Canada: The EU-Canada PNR Agreement

Data-sharing and processing practices are not limited to the European Union and United States. While the United States has been an early player in the field of personal data processing for security purposes, other countries are developing that capacity and their number is likely to increase in the coming years and decades. This gives the current development of a data-protection framework within the European Union particular importance, since the framework would apply to any future agreements negotiated.

89 Article 9(1), Agreement on Mutual Legal Assistance between the European Union and the United States of America.

90 See Paul De Hert and Bart De Schutter," International Transfers of Data in the Field of Jha: The Lessons of Europol, PNR and Swift," in *Justice, Liberty and Security: New Challenges for EU External Relations*, eds. Bernd Martenczuk and Servaas van Thiel (Brussels: VUB Press, 2008).

91 For a review of the agreement and its relation to other EU-related instruments, as well for an overview of the main actors and issues of criticism, see Rocco Bellanova, "The Case of the 2008 German-US Agreement on Data Exchange: An Opportunity to Reshape Power Relations?" in *Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert (Dordrecht, The Netherlands: Springer, 2010).

92 DHS, "Agreement between the Government of the United States of America and the Government of the Federal Republic of Germany on Enhancing Cooperation in Preventing and Combating Serious Crime," (Washington, DC: DHS, 2008), hereinafter: US-German agreement. The so-called Prüm Treaty is an international treaty signed in 2005 by seven EU Member States, outside the official framework of EU cooperation. Part of the cross-border cooperation designed there was lately integrated at the EU level via a European Council decision, and applies to all Member States. A short presentation of the DNA and biometrics exchange foreseen in these instruments is offered in the following section.

While it is out of the scope of this report to offer an overview of similar practices adopted by other countries, it seems worth briefly introducing similar measures that involve Canada.

Following the EU-US PNR agreement, similar discussions opened between the European Union and Canada. The EU-Canada PNR agreement, while under discussion before 9/11, was implemented only in 2005.[93] This delay was the result of negotiations aiming to ensure the "adequacy" of Canada's data-protection laws. Canadian processing of PNR data is not limited to combating terrorism; instead, the Canadian Border Services Agency (CBSA) "will use API *and* PNR information collected from European and other carriers only to identify persons at risk to import goods related to, or persons who are inadmissible to Canada because of their potential relationship to, terrorism or terrorism-related crimes, or other serious crimes, including organized crime, that are transnational in nature."[94]

It should be noted that the Canadian agreement shares many of the essential features of the EU-US agreement: the processing of the commercial data of all passengers, as well as the retention (even if for a more limited period) of the same data. The profiling (risk-assessment) rationale remains the same, as does the broader purpose of the PNR processing. The agreement between the European Union and Canada includes both PNR and API data, while in the United States the use of API remains unilateral (not governed by any agreement). All in all, Canadian authorities collect some 25 fields of data, retained for a maximum of 3.5 years (six years in the case of "interesting" persons).[95]

VI. Conclusion: The Challenges Ahead

Programs for analyzing passenger data have developed more slowly in the European Union than in the United States, although substantial developments have occurred on both sides of the Atlantic in recent years. Different systems for identifying and processing data have developed in tandem or in parallel. Furthermore, other countries, such as Canada, are adopting similar practices. The sheer volume of data collected and the fact that much of the information can be supplied in advance have allowed governments to shift the enforcement focus towards individuals, rather than sorting travelers more narrowly by nationality.

Data-sharing agreements have played a significant role both in enabling these developments to take place, and in limiting potential negative consequences for individuals. European Commission mandates to negotiate new PNR agreements with the United States, Canada, and Australia, and the EU-US data-protection framework agreement have already been adopted, meaning that a new negotiating period is coming up. Among the issues that have attracted the most attention during data-sharing debates is the availability of judicial redress for EU citizens. Also high on the list: The role of independent data-protection authorities (given the recent ECJ judgments on this topic) as well as data-retention time limits and respect for the principle of proportionality. Those are only some of the pending issues that deserve attention during future negotiations; others are also likely to emerge.

The symbolic and practical significance of data-processing and data-protection measures for Member States' agencies, and the growing attention they have received in public debates have served to emphasize possible lines of disagreement within and between the United States and the European Union. The core of the transatlantic disagreement, while sometimes seen as a demonstration of simple

93 EC, "Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency," *Official Journal of the European Union* L091, 29/03/2006 49ff. See Opinion 3/2004 of Article 29 of the Data Protection Working Party; however, the Canadian API/PNR Program appears to have been initiated on October 25, 2001.

94 EC Decision of September 6, 2005, Article 2 of the "Commitments by the Canada Border Service Agency in Relation to the Application of its PNR Program," http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:01:EN:HTML.

95 Ibid., Article 8.

distrust, internal political tensions, or fundamental differences in the understanding of the role of state power on either side of the Atlantic, probably result more from institutional and legal differences in how common principles are implemented in practice.

Recommendations

Technologies and technological choices are socially and politically relevant; technology is not a mere tool that allows policymakers to solve a given issue, but can become an issue in itself. The nature of data-processing practices not only creates unforeseen problems, but has implications for the constitution of societies themselves (e.g., the potential for discrimination, lack of respect for due process, or failure to presume innocence). Even data-retention periods or the scope of data collection without prior suspicion of criminal activity have important effects, including the stigmatization of innocent individuals, chilling effects on social activities perceived to be under continuous surveillance, or the risk that stored data could be stolen or misused.[96]

Of course, we must not refuse to make use of data and technology, but the policies that govern their use require careful design and oversight. Among them should be enforceable limits on how government agencies use personal data, and mechanisms for individuals to assert their rights to privacy and data protection. The EU-US High Level Contact Group on information sharing and privacy acknowledged important pending issues and helped to propose some solutions. Its preference for a binding agreement between the European Union and the United States on data protection in the field of law enforcement, and the positive reception by authorities on both sides of the Atlantic, suggest that real efforts are being made to take data-processing practices seriously. Meanwhile, the EU Commission's draft mandate for negotiations on data protection confirms this tendency, promoting principles such as limited data retention and even presents innovative solutions such as data minimization and compensation.

As noted earlier, individuals are rarely compensated for erroneous decisions made by governments on the basis of data use or misuse. Introducing a consumer law perspective into the debates over the control of human mobility would not only allow individuals to receive compensation where they have suffered harm, but would also foster a more accurate review of the role of data-processing systems and their efficiency, leaving a public record of their use. A consumer law perspective could also reinforce the view that cooperation among countries in dealing with human mobility is generally accepted insofar as it creates tangible advantages for individuals rather than simply expands surveillance. While the EU Commission's draft negotiating mandate envisages judicial redress and compensation, it will be critical to implement these measures effectively and ensure that they provide meaningful protection.

In July 2010, the European Commission proposed two sets of principles for the future adoption of new transatlantic data-related initiatives and for the evaluation of current ones.[97] What the European Commission deems substantive principles are those that concern the safeguard of fundamental rights, necessity, subsidiarity, and accurate risk management.[98] On the other hand, "process-oriented principles" are those involving cost effectiveness, bottom-up policy design, clear allocation of responsibilities, and review and sunset clauses.[99] The decision to list, clarify, and adopt as guidelines, these principles can be welcomed as an important step. However, the principle of "risk management" remains ambiguous. The European Commission should clarify its position on data-profiling techniques

96 Rocco Bellanova and Paul De Hert, "Le Cas S. Et Marper Et Les Données Personnelles : L'horloge De La Stigmatisation Stoppée Par Un Arrêt Européen," *Cultures & Conflits* 76 (2009); Daniel J. Steinbock, "Data Matching, Data Mining, and Due Process," *Georgia Law Review* 40, no. 1 (2005); Paul De Hert, "Balancing Security and Liberty within the European Human Rights Framework: A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11," *Utrecht Law Review* 1, no. 1 (2005).

97 EC, "Communication from the Commission to the European Parliament and the Council. Overview of Information Management in the Area of Freedom, Security and Justice" COM(2010) 385 final, www.statewatch.org/news/2010/jul/eu-com-overview-information-management-com-385-10.pdf.

98 Ibid., 25-26.

99 Ibid., 26-27.

and their role in proposed measures such as the EU PNR or registered-traveler programs.

Data-protection policies have limits in their ability to prevent negative consequences for individuals. First, they can become meaningless if they are accompanied by extensive exemptions. But more fundamentally, they can be reduced to a kind of "procedural checklist" of actions that a government agency must or must not take when using data — and one that can fail to take into account more fundamental questions about whether the very use of certain kinds of data violates the right to privacy.[100] Such a minimal approach to data protection also curtails its ability to "seal" the data-processing machines from uncontemplated or undesired uses and make the powerful accountable.[101]

The nature of data-processing practices not only creates unforeseen problems, but has implications for the constitution of societies themselves.

With this in mind, the final recommendation of this report is to "bring transparency into the machines," in other words to ensure that the full consequences of data use receive public scrutiny and attention. In order to facilitate public and political debates concerning present and future data-collection and sharing measures, for example, the European Commission could request the systematic and regular drafting of privacy and data-protection assessments, including a clear description of the actual use and functioning of relevant technologies. Acknowledging errors and misuses could enable greater democratic control over the data initiatives while fostering trust in the models chosen.

Finally, the public conversation should address nondiscrimination, due process, and the presumption of innocence. The choice of technological architecture affects the likelihood of negative impacts on individuals, and new data systems can be designed with the explicit purpose of limiting any negative effects of this kind.

100 Such a shift is particularly evident in the privacy and data-protection assessment of PNR practices undertaken by the European Commission in its proposal for a global approach to PNR transmission. While at the beginning the European Commission recalls the need to respect the essence of fundamental rights, it finally elaborates a framework that relies only on fair information practices, and even provides for important derogations when core principles of the fundamental right of data protection are at stake. See EC, "Communication from the Commission. On the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries," 7-9.

101 For an elaboration of this point, see De Hert and Gutwirth, "Regulating Profiling in a Democratic Constitutional State," 275.

Works Cited

Aguilar, David V. 2010. Testimony of Acting Deputy Commissioner, US Customs and Border Protection, before the Senate Homeland Security and Governmental Affairs Committee. *The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening*. 111th Cong., 2nd sess., March 10, 2010, 4-7. www.cbp.gov/linkhandler/cgov/newsroom/congressional_test/holiday_attack.ctt/holiday_attack.pdf.

Anderson, Ross, Ian Brown, Terri Dowty, Philip Inglesant, William Heath, and Angela Sasse. 2009. *Database State*. York, UK: The Joseph Rowntree Reform Trust Ltd., 2009.

Archick, Kristin. 2010. *U.S.-EU Cooperation against Terrorism*. Washington: Congressional Research Service. www.fas.org/sgp/crs/row/RS22030.pdf.

Bellanova, Rocco. 2010. The Case of the 2008 German-US Agreement on Data Exchange: An Opportunity to Reshape Power Relations? In *Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert. Dordrecht, The Netherlands: Springer.

Bellanova, Rocco, and Paul De Hert. 2009. Le Cas S. Et Marper Et Les Données Personnelles : L'horloge De La Stigmatisation Stoppée Par Un Arrêt Européen. *Cultures & Conflits* 76: 101-14.

Bignami, Francesca. 2007. European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review* 48: 609-98.

Brouwer, Evelien. 2009. The EU Passenger Name Record System and Human Rights: Transferring Passenger Data or Passenger Freedom? In *CEPS Working Document*. Brussels: The Centre for European Policy Studies.

Cody, Edward. 2010. Armed with New Treaty, Europe Amplifies Objections to U.S. Data-Sharing Demands. *The Washington Post*, October 26, 2010.

Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. 2006. *Report of the Events Relating to Maher Arar*. Ottawa: Gilmore Print Group.

Council of the European Union. 2008. *EU US Summit, 12 June 2008. Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection*. Brussels: Council of the European Union.

_____. 2010. 3034th Council Meeting, Justice and Home Affairs. Press release, October 7-8, 2010. Luxembourg: Council of the European Union.

_____. 2010. 3051st Council Meeting, Justice and Home Affairs. Press release, December 2-3, 2010. Luxembourg: Council of the European Union.

_____. 2010. *The Stockholm Programme - an Open and Secure Europe Serving and Protecting Citizens*. Brussels: Council of the European Union.

_____. 2010. *Draft Internal Security Strategy for the European Union: Towards a European Security Model*. Brussels: Council of the European Union.

De Busser, Els. 2010. EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal? *Utrecht Law Review* 6, no. 1: 86-100.

De Hert, Paul. 2005. Balancing Security and Liberty within the European Human Rights Framework: A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11. *Utrecht Law Review* 1, no. 1: 68-96.

De Hert, Paul and Rocco Bellanova. 2008. *Data Protection from a Transatlantic Perspective: The EU and US Move Towards an International Data Protection Agreement?* Brussels: European Parliament's Committee on Civil Liberties, Justice and Home Affairs.

De Hert, Paul and Bart De Shutter. 2008. International Transfers of Data in the Field of Jha: The Lessons of Europol, PNR and Swift. In *Justice, Liberty and Security: New Challenges for EU External Relations*, eds. Bernd Martenczuk and Servaas van Thiel. Brussels: VUB Press.

De Hert, Paul and Serge Gutwirth. 2008. Regulating Profiling in a Democratic Constitutional State. In *Profiling the European Citizen. Cross Disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth. Dordrecht: Springer.

De Hert, Paul and Vagelis Papakonstantinou. 2010. The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe. *Computer Law & Security Review* 26.

Department of Homeland Security (DHS). 2007. Advance Electronic Transmission of Passenger and Crew Member Manifests for Commercial Aircraft and Vessels Final Rule. *Federal Register,* 48320-45.

_____. 2008. Agreement between the Government of the United States of America and the Government of the Federal Republic of Germany on Enhancing Cooperation in Preventing and Combating Serious Crime. Washington, DC: DHS.

DHS Privacy Office. 2009. *2009 Data Mining Report to Congress*. Washington, DC: DHS. www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.

Electronic Privacy Information Center (EPIC). Air Travel Privacy. Accessed December 13, 2010. http://epic.org/privacy/airtravel/.

_____. 2006. *Privacy and Human Rights: An International Survey of Privacy Laws and Developments*. Washington: EPIC and Privacy International.

European Commission (EC). 2001. Regulation (Ec) No 539/2001 Listing the Third Countries Whose Nationals Must Be in Possession of Visas When Crossing the External Borders of Member States and Those Whose Nationals Are Exempt from That Requirement. *Official Journal of the European Union*," 1-7, 2001.

_____. 2004. Council Directive 2004/82/Ec of 29 April 2004 on the Obligation of Carriers to Communicate Passenger Data, Article 1. *Official Journal of the European Union*.

_____. 2005. Commission Decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency. *Official Journal of the European Union* L091, 29/03/2006 49ff. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:091:0049:01:EN:HTML.

_____. 2007. Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes. Brussels: EC.

_____. 2008. Regulation (Ec) No 767/2008 of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (Vis) and the Exchange of Data between Member States on Short-Stay Visas (Vis Regulation)." *Official Journal of the European Union*: 60-81.

_____. 2008. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the Next Steps in Border Management in the European Union. Brussels: EC.

_____. 2008. Regulation (Ec) No 767/2008 of the European Parliament and of the Council of 9 July 2008 Concerning the Visa Information System (Vis) and the Exchange of Data between Member States on Short-Stay Visas (Vis Regulation).

_____. 2010. Communication from the Commission to the European Parliament and the Council. Overview of Information Management in the Area of Freedom, Security and Justice. Brussels: EC.

_____. 2010. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an Area of Freedom, Security and Justice for Europe's Citizens. Action Plan Implementing the Stockholm Programme. Brussels: EC.

_____. 2010. Communication from the Commission on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries. *Official Journal of the European Union*, December 30, 2010.

_____. 2010. Proposition De Recommandation Du Conseil Autorisant L'ouverture De Negociations En Vue D'un Accord Entre L'union Européenne Et Les États-Unis D'Amérique Sur La Protection Des Données Personnelles Lors De Leur Transfert Et De Leur Traitement À Des Fins De Prevention, D'investigation, De Detection Ou De Poursuite D'Actes Criminels Y Compris Le Terrorisme, Dans Le Cadre De La Cooperation Policiaire Et Judiciaire En Matiere Penale. Brussels: EC.

Official Journal 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) L204/17, August 4, 2007.

_____. 2008. Treaty on the Functioning of the European Union (TFEU). May 9, 2008, C 115, 49-199.

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, no. 3: 885-919.

Pawlak, Patryk. 2009. *Made in the USA? The Influence of the US on the EU's Data Protection Regime*. Brussels: Centre for European Policy Studies.

Pérez Asinari, Maria Veronica and Pablo Palazzi, eds. 2008. *Défis Du Droit À La Protection De La Vie Privée-Challenges of Privacy and Data Protection Law*. Brussels: Bruylant.

Privacy International. Border and Travel Surveillance. Accessed December 13, 2010. www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Border+and+Travel+Surveillance&als[theme]=Border%20and%20Travel%20Surveillance&conds[1][category.....]=Border%20and%20Travel%20Surveillance.

Rubinstein, Ira S., Ronald D. Lee, and Paul M. Schwartz. 2008. Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review* 75, no. 1: 261-85.

S. And Marper V. The United Kingdom. 2008.

Statewatch. Observatory on the Exchange of Data on Passengers (PNR) with USA. Accessed March 2, 1011. www.statewatch.org/pnrobservatory.htm.

State Department. Visa Waiver Program (VWP). Accessed March 2, 2011. http://travel.state.gov/visa/temp/without/without_1990.html#vwp.

Steinbock, Daniel J. 2005. Data Matching, Data Mining, and Due Process. *Georgia Law Review* 40, no. 1: 1-86.

Tanaka, Hiroyuki, Rocco Bellanova, Susan Ginsburg, and Paul De Hert. 2010. *Transatlantic Information Sharing: At a Crossroads*. Washington, DC: Migration Policy Institute.

Valverde, Mariana and Michael S. Mopas. 2004. Insecurity and the Dream of Targeted Governance. In *Global Governmentality*, eds. Wendy Larner and William Walters. New York: Routledge.

White House. 2010. *National Security Strategy*. Washington, DC: White House. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Whitman, James Q. 2004. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Public Law & Legal Theory Research Paper Series* no. 64: 1-94.

Muller, Benjamin J. 2010. *Security, Risk and the Biometric State: Governing Borders and Bodies*. Eds. Peter J. Burgess, Prio New Security Studies. London/New York: Routledge.

Official Journal 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) L204/17, August 4, 2007.

_____. 2008. Treaty on the Functioning of the European Union (TFEU). May 9, 2008, C 115, 49-199.

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, no. 3: 885-919.

Pawlak, Patryk. 2009. *Made in the USA? The Influence of the US on the EU's Data Protection Regime*. Brussels: Centre for European Policy Studies.

Pérez Asinari, Maria Veronica and Pablo Palazzi, eds. 2008. *Défis Du Droit À La Protection De La Vie Privée-Challenges of Privacy and Data Protection Law*. Brussels: Bruylant.

Privacy International. Border and Travel Surveillance. Accessed December 13, 2010. www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Border+and+Travel+Surveillance&als[theme]=Border%20and%20Travel%20Surveillance&conds[1][category.....]=Border%20and%20Travel%20Surveillance.

Rubinstein, Ira S., Ronald D. Lee, and Paul M. Schwartz. 2008. Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches. *The University of Chicago Law Review* 75, no. 1: 261-85.

S. And Marper V. The United Kingdom. 2008.

Statewatch. Observatory on the Exchange of Data on Passengers (PNR) with USA. Accessed March 2, 1011. www.statewatch.org/pnrobservatory.htm.

State Department. Visa Waiver Program (VWP). Accessed March 2, 2011. http://travel.state.gov/visa/temp/without/without_1990.html#vwp.

Steinbock, Daniel J. 2005. Data Matching, Data Mining, and Due Process. *Georgia Law Review* 40, no. 1: 1-86.

Tanaka, Hiroyuki, Rocco Bellanova, Susan Ginsburg, and Paul De Hert. 2010. *Transatlantic Information Sharing: At a Crossroads*. Washington, DC: Migration Policy Institute.

Valverde, Mariana and Michael S. Mopas. 2004. Insecurity and the Dream of Targeted Governance. In *Global Governmentality*, eds. Wendy Larner and William Walters. New York: Routledge.

White House. 2010. *National Security Strategy*. Washington, DC: White House. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Whitman, James Q. 2004. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Public Law & Legal Theory Research Paper Series* no. 64: 1-94.

About the Authors

Paul De Hert is an international human-rights expert, specializing in criminal law and technology and privacy law. At the Vrije Universiteit Brussel, he holds the chairs of Criminal Law, International and European Criminal Law, and Historical Introduction to Eight Major Constitutional Systems. He is Director of the university's Research Group on Fundamental Rights and Constitutionalism, Director of the Department of Interdisciplinary Studies of Law (Metajuridics), and is a core member of the internationally respected research group, Law Science Technology & Society. At Tilburg University, he is Associate Professor in the Institute of Law and Technology.

He is a member of the editorial boards of several national and international scientific journals, including the *Inter-American and European Human Rights Journal*, and *Criminal Law & Philosophy*. He is coeditor-in-chief of the *Supranational Criminal Law Series* and the *New Journal of European Criminal Law.*

Rocco Bellanova is a Researcher of the Centre de Recherche en Science Politique at the Facultés universitaires Saint-Louis and of the Law, Science, Technology and Society research group of the Vrije Universiteit Brussel.

His main research interest (and ongoing PhD) focuses on the politics of data protection, and in particular on their impact on security and surveillance practices. Currently, his work is focusing in two areas: transatlantic relations dealing with data processing and data protection; and the role of technologies in the making of the European Union Justice and Home Affairs.

For more on the Improving US and EU Immigration Systems Project, please visit:
www.migrationpolicy.org/immigrationsystems

The Migration Policy Institute is a nonprofit, nonpartisan think tank dedicated to the study of the movement of people worldwide. MPI provides analysis, development, and evaluation of migration and refugee policies at the local, national, and international levels. It aims to meet the rising demand for pragmatic and thoughtful responses to the challenges and opportunities that large-scale migration, whether voluntary or forced, presents to communities and institutions in an increasingly integrated world.

www.migrationpolicy.org

1400 16th Street NW
Suite 300
Washington, DC 20036

Tel: 001 202-266-1940
Fax: 001 202-266-1900