TRANSATLANTIC INFORMATION SHARING: AT A CROSSROADS

Hiroyuki Tanaka
Migration Policy Institute

Rocco Bellanova
Vrije Universiteit Brussel & Facultés universitaires Saint-Louis

Susan Ginsburg
Migration Policy Institute

Paul De Hert
Vrije Universiteit Brussel & Tilburg University

January 2010

Acknowledgments

The authors thank the participants of two private roundtables hosted in 2009 by the Migration Policy Institute (MPI) with the support of the Delegation of the European Union to the United States. The first roundtable, held in London in partnership with the International Institute for Strategic Studies on January 15-16, 2009, convened 24 US, EU, and European experts to discuss the future of visa-free travel and international registered-travel programs. The second roundtable, held in Detroit, Michigan on April 14-16 with additional support from the Heinrich Böll Stiftung North America, brought together 35 US, EU, and European government and private experts, including some members of the High Level Contact Group, on security-related information-sharing programs and agreements.

The authors also thank Mark Koumans, Bob Mocny, Mary Ellen Callahan, John Kropf, Valerie Wood, and Robert Neuman of the US Department of Homeland Security, as well as Ken Propp of the US Department of State and Frank Schmiedel of the Delegation of the European Union to the United States for providing valuable insights and information.

Finally, the authors would like to thank Michelle Mittelstadt and Liliana Luper of MPI for their excellent editing and comments.

MPI is grateful for the generous support of the Delegation of the European Union to the United States and the Heinrich Böll Stiftung North America, which made this report possible. This is the final report of *Building a Secure Transatlantic Space for the 21st Century*, a two-year project sponsored by the Delegation of the European Union to the United States that enabled MPI to explore important contemporary transatlantic mobility and security issues. The recommendations in this report are solely those of the authors.

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

Table of Contents

Executive Summary

The 9/11 terrorist attacks and the subsequent Madrid and London bombings sparked a sense of urgency (reinvigorated by the attempted Christmas Day 2009 attack on a US airliner) on the part of US and European governments to stop terrorists from committing more acts of indiscriminate violence. This report focuses on one area in which the United States and the European Union (EU) have stepped up cooperation in the fight against terrorism and crime: information sharing relating to human mobility.

Since Sept. 11, 2001, one of the key counterterrorism policies of the United States and the European Union has been to require air carriers, governments, and individuals to submit to relevant authorities commercial, law enforcement-related, or personal information on travelers. With this information, governments vet all individuals intending to travel internationally against government watch lists and databases on known or suspected terrorists, criminals, and lost and stolen passports as well as travel pattern algorithms to screen for potential threats.

The promise of these technologies and practices is to help government agencies mitigate risk by tracking and detecting threats in advance and to comply with their mission in a safer and more efficient way. While the recourse to these technologies has allowed governments to "export the border," — dealing with threats abroad in cooperation with foreign authorities instead of confronting them at home (or en route) — the effectiveness of these measures at detecting and stopping threats abroad or at the border cannot be ascertained fully. A large number of officials from interior and homeland security ministries claim that these measures are effective, but the scarcity of publicly available government data on and the relative lack of legislative branch scrutiny over them make it hard to make an honest assessment about them. And, as the aborted terrorist attack that occurred on an Amsterdam-to-Detroit flight on Christmas Day 2009 demonstrates, human and intelligence-sharing failures bear on the effectiveness of any information-sharing programs.

Nevertheless, governments have made public a few instances in which such databases and information-sharing agreements have enabled them to stop unwanted individuals from entering their countries. In 2008, for example, Eurodac — the EU computer database of asylum seekers and individuals apprehended in relation to an illegal crossing or illegal residence — recorded 38,445 multiple asylum applications out of a total 219,557 asylum applications. This means that up to 17.5 percent of asylum applicants had already filed an asylum application in another EU Member State.[1] In 2004, the UK Home Office launched Project Semaphore, which runs passenger name record (PNR) and Advance Passenger Information (API) information against government watch lists for law enforcement and border control purposes. Through this project, the United Kingdom since 2005 has made 4,650 arrests for murder, rape and assault, sexual

[1] The actual proportion is likely to be lower as some EU Member States take fingerprints of failed asylum seekers when they receive them from another EU Member State. See Commission of the European Communities, *Report from the Commission to the European Parliament and to the Council: Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008* (Brussels, Belgium: Commission of the European Communities, 2009), http://www.statewatch.org//news/2009/sep/eu-com-ann-rep-eurodac-2008.pdf.

offenses, kidnap, and document fraud, and has seized false documents, tobacco, and drugs.[2]

It is important to recall, however, that the impetus in the US context for systematically implementing such information-sharing programs in the post-9/11 world has chiefly been counterterrorism, not law enforcement or immigration control. The entire context for EU-US information-sharing discussions, initiated by the United States, initially has been terrorism prevention. Migration management and crime control elements incorporated into the discussions have been, during this first phase, of particular interest on the European side. Against this security backdrop, governments on both sides of the Atlantic are using information that individuals voluntarily provide about themselves to facilitate and expedite international travel. Most notably, biometric, technology-based registered traveler programs in the United States and across Europe offer pre-vetted individuals expedited clearance at security and immigration checkpoints.

The twin objectives of simultaneously securing and facilitating international travel have steered the United States and the European Union to place high value on the collection, processing, and sharing of personal information. Today, information-sharing programs are widely considered critical intelligence, law enforcement, and mobility risk management tools that help governments combat terrorism and transnational crime.

Despite the benefits of sharing commercial, government, or personal information for law enforcement and intelligence purposes, US and EU officials have struggled to find a mutually satisfactory legal framework for sharing information. A noisy diplomatic row between the United States and the European Union in negotiating the EU-US passenger name record agreement in 2004 illustrates such challenges.

Since 2006, US and EU policymakers have tried to resolve their differences over how to guarantee privacy and personal data protection under their respective legal and institutional settings. The main issues of contention for both sides include: access to administrative and judicial redress procedures, private companies' obligations to share information with governments, the impact of information-sharing agreements on relations with third countries, and the divergent institutional setups of US and EU privacy agencies and their respective oversight powers and privacy guarantees.

In November 2009, an informal working group of US and EU officials and experts, commonly known as the EU-US High Level Contact Group (HLCG) on information sharing and privacy and personal data protection, agreed on a set of nonbinding common principles for sharing information for law enforcement purposes. The goal of HLCG was to explore ways that would enable the European Union and the United States to work more closely and efficiently in exchanging law enforcement information while ensuring the protection of personal data and privacy. The group's identification of the fundamentals or "common principles" of an effective regime for privacy and personal data protection was to be the first step towards that goal. While the United States and the European Union continue to work on establishing a legal framework to share information for law enforcement purposes, the HLCG work has made clear that

[2] Home Office, UK Border Agency, "How we tested e-borders," http://www.ukba.homeoffice.gov.uk/managingborders/technology/eborders/testingeborders/; House of Lords European Union Committee, *The Passenger Name Record (PNR) Framework Decision: Report with Evidence*, 15th Report of Session 2007-08 (London, United Kingdom: The Stationary Office Limited, 2008), http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf.

the definitions of "law enforcement purposes" adopted by the United States and the European Union differ. The United States defines it as the use "for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for noncriminal judicial or administrative proceedings related directly to such offenses or violations," whereas the European Union defines it more narrowly as the use "for the prevention, detection, investigation, or prosecution of any criminal offense."[3] The difference in their definitions is relevant to the extent that different definitions of "law enforcement" implicate different actors, agencies, processes, and types of information.

While the common principles are a step in the right direction, the United States and the European Union have yet to negotiate, draft, and sign a binding international agreement that will govern the sharing of personal information for law enforcement purposes. The entry into force of the Lisbon Treaty on December 1, 2009 implies a shift in how the United States and the European Union will negotiate an agreement and raises questions about how they will shape new practices. Importantly, the treaty introduces new EU legal and institutional frameworks for handling Justice and Home Affairs, presents new political and legal questions on how the Union and its allies will act and cooperate on these matters, and affects current EU legislation and policy on law enforcement, police cooperation, and privacy and data protection.

This report describes and analyzes the legal, privacy, and data-protection frameworks for information-sharing agreements relating to human mobility that enable the United States and the European Union to share such information for law enforcement purposes.

It also examines the various informal and formal channels through which the United States and the European Union have discussed their privacy and personal data-protection concerns. In particular, it traces the work of HLCG and offers policy considerations that would help both sides reach a transatlantic information-sharing agreement. Among the recommendations:

- The United States and the European Union should work toward negotiating a binding international agreement by setting up a roadmap that would help both sides lay out their goals and steps for diplomatic negotiations, while allowing relevant experts not involved in formal negotiations to offer their input.
- The US government should consider establishing a central privacy office. This would assure European officials and experts that the United States has an effective privacy watchdog.
- The US and EU governments should regularly publish annual reports or make public evaluations of the effectiveness of information-sharing agreements and the databases that collect and process information in stopping known or suspected terrorists and criminals from obtaining visas and entering their respective countries.
- The United States and the European Union should update their respective privacy and personal data-protection laws to reflect current security needs. Such laws also should clearly define the application of these laws vis-à-vis foreigners (legal nonpermanent residents and noncitizens).

---

[3] Council of the European Union, *Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection* (Brussels, Belgium: Council of the European Union, 2009), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/report_hlcg_info_sharingprivacydata_prot.pdf.

- The United States and the European Union should consider adding members to HLCG or the group that will likely succeed it to negotiate a binding international agreement.
- Policymakers should educate their publics and legislators about the differences in how the United States and the European Union define sharing information for law enforcement purposes.

Governments already have the technologies and practices to share information on individuals with each other and will most likely introduce and implement others. The outstanding challenge is to how the United States and the European Union can ensure and integrate the best level of privacy and data protection into new practices. Both are at a crossroads for determining the legal framework for exchanging personal information, derived from commercial, government, or individual sources, for law enforcement purposes. How soon the United States and the European Union reach a legal agreement governing the sharing of information on individuals will depend on the willingness of both parties to address and accommodate their differences in protecting privacy and personal information and on the importance attributed to these negotiations by political leadership on both sides.

"The fight against transnational crime and terrorism often requires the sharing of personal data for law enforcement and public security purposes, which compels us to protect the human rights, fundamental freedoms, and civil liberties in all fields of transatlantic cooperation."

EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom, and Security," November 3, 2009

I. Introduction

On November 3, 2009, participants of the United States-European Union Justice and Home Affairs Ministerial meeting released a joint statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom, and Security".[4] The statement and the issuance of a final common set of principles on privacy and personal data protection concluded the work of the High Level Contact Group (HLCG), an informal group set up by the US-EU Justice and Home Affairs Ministerial Troika in 2006 with the goal of facilitating the dialogue on transatlantic privacy, data protection, and data sharing for law enforcement purposes.[5] The joint statement reaffirmed the importance of negotiating a binding international EU-US agreement on these issues. The HLCG is likely to resume negotiations in 2010.

The sharing and processing of personal data for security and mobility management purposes, while freighted with policy, privacy, and law enforcement considerations, is high on the transatlantic policy agenda. Notwithstanding the strong mutual interest in sharing travelers' personal information and fostering international cooperation in the field of law enforcement more generally, the United States and the European Union have raised and encountered several issues and challenges in cooperating and adopting measures to process personal data.

Furthermore, the complex differences between the US and EU legal frameworks and the entry into force of the Lisbon Treaty on December 1, 2009 are presenting new political and legal questions on how the Union and its allies will act and cooperate on matters pertaining to Justice and Home Affairs (JHA).[6] In particular, the Lisbon Treaty profoundly affects EU institutional and legal structures, enhancing roles for the European Parliament and the European Court of Justice (ECJ)[7]; splitting the former European Commission portfolio for Justice, Liberty, and Security into one for Justice, Fundamental Rights, and Citizenship and another for Home Affairs; ending the European Union's pillar structure;[8] and legally integrating the Charter of Fundamental

[4] US Department of Homeland Security, "EU-US Joint Statement on 'Enhancing transatlantic cooperation n the area of Justice, Freedom, and Security,' November 3, 2009,http://www.se2009.eu/polopoly_fs/1.21271!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf.

[5] Council of the European Union, "Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection," November 23, 2009, http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf.

[6] Both the United States and the European Union will likely modify or revise their current legislation on privacy and data protection.

[7] The European Court of Justice, as the highest court in the European Union for matters of EU law, is responsible for interpreting EU law and ensuring its equal application across all Member States.

[8] Prior to the Lisbon Treaty's enactment, the European Union was comprised of three pillars: the first, or community, pillar, corresponding to the European Community, the European Atomic Energy Community, and the former European Coal and Steel Community; the second pillar, devoted to the

Rights of the European Union into EU constitutional rules and principles.[9] These changes will affect current legislation and policy concerning law enforcement and police cooperation, as well as privacy and data protection, especially since several of the most important pieces of legislation will be submitted to these EU institutions for review.[10]

Even as the EU structure is changing, the US government is facing growing calls to update its privacy policies. Several major actors, such as the Defense Department's Technology and Privacy Advisory Committee, the Government Accountability Office, and the Office of Management and Budget (OMB) have expressed their opinion that US privacy legislation must be updated.[11]

Transatlantic cooperation in the fields of legal and security issues is wide in scope. This report focuses on a limited but crucial area, namely transatlantic information sharing on human mobility. As human mobility has increased, it poses a steady challenge to the conceptions and forms of state interventions and responsibilities in the fields of security, migration, rights, and economy. Virtually no country remains untouched by the temporary or permanent movement of people worldwide. In 2008, nearly 925 million international tourist arrivals were recorded globally,[12] and the United Nations estimates that 214 million individuals will be living outside their countries of origin in 2010.[13]

On the one hand, governments and businesses view the international movement of people — tourists, workers of all skill levels, and students — as a precious economic resource; on the other, policymakers also see it as a security risk in the context of transnational crime and terrorism. Furthermore, while the majority of unauthorized migrants and visa overstays do not pose a security risk in the terrorism or transnational crime contexts, they challenge a country's ability to effectively administer the laws that govern its immigration policy.

In both the United States and the European Union, policymakers have often overly securitized the issue of managing migration. In the United States, political debates and immigration legislation have focused primarily on a crackdown on illegal immigration, and the Department of Homeland Security (DHS) was established with the overriding

---

common foreign and security policy; and the third pillar, devoted to police and judicial cooperation in criminal matters.

[9] However, the Lisbon Treaty does not necessarily initiate all changes that occur after its enactment. For example, plans to revise the EU data protection directive existed several years prior to the Lisbon Treaty's effective date. The Lisbon Treaty will nevertheless provide impetus for adopting a new data protection directive with fresh scope and meaning under its new legal framework. The outcome and effective scope of such changes remain unclear. This report refers to first, second, and third pillars of the European Union as they applied to areas and actors prior to Lisbon Treaty enactment.

[10] The Mutual Legal Assistance Treaty will not be submitted for review since it was ratified by all EU Member States prior to enactment of the Lisbon Treaty.

[11] US authorities have called for updates to current US privacy law and policy. These authorities include: the Defense Department's Technology and Privacy Advisory Committee in 2004, the National Research Council's Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals in 2008, the Government Accountability Office and Secretary of Commerce's Information Security and Privacy Board in 2008, and in 2009, the Director of the Office of Management and Budget and the Director of the National Security Agency.

[12] Jennifer Blanke and Thea Chiesa, *The Travel & Tourism Competitiveness Report 2009: Managing in a Time of Turbulence.* (Geneva: World Economic Forum, 2009), http://www.weforum.org/pdf/ttcr09/ttcr09_fullreport.pdf.

[13] United Nations, Department of Economic and Social Affairs, Population Division, *Trends in International Migrant Stock: The 2008 Revision*, http://esa.un.org/migration/p2k0data.asp.

focus of protecting the country against terrorist attack. EU policymakers have politicized the issue of clamping down on bogus asylum seekers and unauthorized immigrants in the context of security passing national legislation that simultaneously addresses immigration and transnational crime.

By sharing information on travelers, governments are trying to help each other mitigate risk and tackle threats stemming from organized crime, terrorism, and other dangerous and illicit activities, while facilitating travel for *bona fide* travelers.

II. Political and Legal Context for Transatlantic Data Sharing and Processing

A. Why Governments Want to Share Information on Travelers

Since the 9/11 attacks, governments have become increasingly interested in sharing information on travelers with each other, though, of course, government interest and international cooperation in this area predated September 2001.

The collection, storage, processing, and exchange of personal data were not completely novel policies for governments and already were considered crucial tools in managing populations, maintaining the public order, and securing and facilitating travel.[14] A tradition of international cooperation in these fields was already established both within Europe (see the TREVI Group)[15] and within the G-7 (later G-8, and soon-to-be G-20). (See the Roma-Lyon Group).[16] Indeed, exchange of personal data goes back further in time and can be linked to wider processes of mobility and international trade and commerce. Interpol, for example, dates back to 1914 when an International Criminal Police Congress brought together police officers, lawyers, and magistrates from 14 countries to discuss cooperative arrest procedures, identification techniques, centralized international criminal records, and extradition.[17] Even before then, states concluded bilateral agreements to facilitate the extradition of convicts and criminal suspects, as well as the sharing of associated investigative information.[18]

In the post-9/11 era governments have exhibited a renewed interest in measures that allow them to share personal data with each other, especially those that integrate new technologies enabling them to control the flow of people, goods, and finances at a

[14] For example, European governments have expanded the use of ID documents or allowed wiretapping for intelligence purposes. The United States used passenger name record (PNR) and Automated Targeting System (ATS) prior to 9/11, while the European Union had set up the Schengen Information System and EURODAC.
[15] Sandra Lavenex, "Justice and Home Affairs: Towards a European Public Order?" in Helen Wallace, William Wallace, and Mark Pollack, eds., *Policy-Making in the European Union: Fifth Edition* (Oxford: Oxford University Press, 2005), 457-480.
[16] Ian Hosein, "The Sources of Laws: Policy Dynamics in a Digital and Terrorized World," *The Information Society*, 20 (2004): 187-199.
[17] Interpol, "A brief history of INTERPOL,"
http://www.interpol.int/public/ICPO/Governance/SG/history.asp.
[18] See, for example, Gary Botting, *Extradition Between Canada and the United States* (Ardsley, NY: Transnational Publishers, Inc., 2005).

distance (both in temporal and spatial terms, or "exporting" the border).[19] Terrorist attacks and foiled plots in the European Union have also pushed countries to adopt or broaden a variety of security measures.[20]

While we can only speculate whether the United States could have prevented the 9/11 attacks, the failure of different agencies within the US government to share already known information on the 9/11 hijackers and their travel documents has been identified as having likely facilitated the execution of the attacks (see report of the National Commission on Terrorist Attacks Upon the United States, known as the 9/11 Commission).[21] The fixes for those intelligence-sharing failures have come under sharp review recently in the wake of the attempted Christmas Day 2009 takedown of a US airliner, allegedly by a Nigerian suspected of affiliation with al Qaeda elements in Yemen.

B. Purposes of Information Sharing and Processing

The US and European governments currently share information on travelers to better secure, manage, and facilitate the international movement of people. The United States and EU Member States have framed virtually all of their information-sharing agreements relating to human mobility in the context of strengthening security against "dangerous individuals" and facilitating travel for low-risk individuals.

In this context, governments obtain and analyze data on travelers for two major reasons: (1) for traditional security purposes such as countering terrorism and combating organized crime that has become more international in nature; and (2) for human mobility-related purposes, such as managing travel and immigration.

Governments process information on travelers — including information contained in a visa application, the biographical page of a passport, the biometric chip of an electronic passport, the biometric digital facial picture and fingerprints submitted to immigration authorities upon arrival at a port of entry, the details included in flight reservations, credit card numbers, frequent flyer miles, and meal preferences — for at least five major purposes.

First, biographical and biometric information on individuals as well as information on their travel documents and travel patterns can serve as a useful counterterrorism and crime-fighting tool. When an individual appears at a consulate for a visa interview or a port of entry to seek admission to a country, government officials electronically scan information that an individual provides against terrorist and criminal watch lists to identify known or suspected dangerous individuals. Importantly, policymakers have made a paradigmatic, and sometimes controversial, shift in emphasis away from investigating committed crimes to taking proactive measures against threats based on risk-assessment methods previously used more for intelligence purposes. The expanded

[19] Today, we see a new form of terrorism, frequently defined as global and networked. This analysis reinforced the post-Cold War interest in building and relying on more "de-territorialized" forms of security systems and border controls.

[20] For example, the European Union adopted the Advance Passenger Information directive in the aftermath of the Madrid attacks and the EU Data Retention directive after the London attacks.

[21] National Commission on Terrorist Attacks Upon the United States, *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States* (Hillsboro Press: 2004), http://www.9-11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf.

use of algorithms, data mining, and profiling programs developed to enhance national security is neither a neutral nor undisputed government practice.

Even within the national security community there are debates about appropriate limits and safeguards for use of these methods. One of the challenges for the United States and the European Union is to clarify and build up the law governing the collection and sharing of information for intelligence and information purposes, including for counterterrorism, law enforcement, and border screening purposes.

These programs have sparked criticism for intrusive techniques that reveal private information and for their inefficiency in tackling transnational crime or terrorism.[22] Government collection and processing of data in such ways raises two major concerns. First, the transfer and processing of bulk data such as Passenger Name Records (PNR) — commercial information on passengers that is created, collected, and stored by airlines in their computer reservation systems or a global distribution system when travelers book their travel — raises more privacy and data-protection concerns than that of *ad hoc*, case-by-case data where the latter involves limited surveillance based on evidence. These data-mining or profiling techniques often rely on private-sector companies to actively or passively supply governments with commercial information and software, and sometimes even the human resources to process information. The role of the private sector in supplying and processing data for law enforcement purposes should be better regulated and understood. The United States also shares information on known or suspected terrorists (watch lists) with at least 17 countries under Homeland Security Presidential Directive 6 to support private and public screening processes and help government officials in the diplomatic, military, intelligence, law enforcement, and immigration communities make better informed decisions.[23]

Second, just as biographical and biometric information provided by individuals can help prevent or monitor the international movement of terrorists it can also serve as a political or diplomatic tool to help prevent human-rights violators and other politically designated individuals from obtaining a visa or entering a country. For example, since 1985 the United States has issued at least 17 presidential proclamations banning selected individuals or groups from traveling to the country.[24]

Third, the United States and Europe share with each other and leverage information for immigration enforcement. Information on travelers can help prevent admission to those seeking to enter a country illegally by using fraudulent or altered genuine travel documents or seeking asylum in multiple countries. The recently signed High-Value Data-Sharing Protocol among the immigration authorities of the Five Country

---

[22] Daniel J. Solove, "Data Mining and the Security-Liberty Debate," *The University of Chicago Law Review*, 75, 1 (2008), 343-362; 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, 1 (2008), 261-285; Daniel J. Steinbock, "Data Matching, Data Mining, and Due Process," *Georgia Law Review*, 40, 1 (2005), 1-86.

[23] US Department of Homeland Security, "Homeland Security Presidential Directive 6: Directive on Integration and Use of Screening Information to Protect Against Terrorism," August 25, 2008, http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm.

[24] For example, Proclamation 5377 (October 4, 1985) suspended the entry as nonimmigrants of Cuban government or Communist Party officers or employees in response to Cuba's disruption of regular US-Cuban migration procedures, while Proclamation 5887 (1988) suspended the entry as visitors of Nicaraguan government officers and employees as a response to Nicaragua's expulsion of eight US diplomats.

Conference[25] will allow the United Kingdom, Canada, the United States, Australia, and New Zealand to share fingerprint information of foreign criminals and asylum seekers in order to detect individuals with previous criminal histories in their countries, expedite removals, and establish previously unknown identities.[26]

Biometric-based entry-exit systems at ports of entry, which record when an individual enters or leaves a country, also allow immigration authorities to detect visa overstays. People who try to abuse or violate immigration laws are less likely to succeed if governments have biographical and biometric information on previous offenders of immigration law or asylum seekers who have unsuccessfully sought asylum in other countries.

Fourth, information-sharing agreements enable countries to conduct law enforcement activities such as extradition or joint criminal investigations on wanted individuals. When the EU-US agreements on extradition and mutual legal assistance enter into force in early 2010,[27] they will allow the United States and the European Union to set up joint investigation teams, utilize video teleconferencing technology to hear testimonies, and respond promptly to requests for accessing bank and other financial records of suspects.[28]

Lastly, governments collect and share information on travelers to facilitate and expedite travel for *bona fide* and registered travelers. The Netherlands and the United Kingdom, for example, have successfully rolled out their respective iris-based systems — Privium and IRIS — while the United States recently launched its fingerprint-based Global Entry. Governments will begin partnering with each other to offer their respective national registered travel programs to their citizens. For example, under a pilot known as the Fast Low Risk Universal Crossing (FLUX) Alliance, the United States and the Netherlands allow US citizens who become Global Entry members to apply for the Dutch Privium program so that they may enjoy the benefits of both registered traveler programs.[29]

---

[25] Home Office, UK Border Agency, *Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference*, August 2009, http://www.bia.homeoffice.gov.uk/sitecontent/documents/managingourborders/strengthening/pia-data-sharing-fcc.pdf.

[26] The pilot version of this program revealed that an individual who sought asylum in the United Kingdom as a Somali had been fingerprinted in the United States while traveling on an Australian passport. Australia confirmed that the asylum seeker was an Australian citizen wanted for rape, which resulted in his deportation to Australia.

[27] US Department of Justice, "Attorney General Holder Speaks at EU/US Justice and Home Affairs Ministerial Meeting," (speech, Washington, DC, October 28, 2009), http://www.justice.gov/ag/speeches/2009/ag-speech-091028.html; Official Journal of the European Union, "Agreement on mutual legal assistance between the European Union and the United States of America," July 19, 2003, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF; Official Journal of the European Union, "Agreement on extradition between the European Union and the United States of America," July 18, 2003, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0027:0033:EN:PDF.

[28] According to the Joint EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom and Security," of November 2009, an EU-US working group will promote the implementation of the agreements and the US and European governments will plan seminars to help practitioners learn how to implement and monitor their provisions.

[29] US Department of Homeland Security, Customs and Border Protection, "Global Entry with Expedited Entry into the Netherlands," May 5, 2009, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/global_entry_flux.xml.

C. Legal Frameworks that Allow Governments to Collect and Share Information

National Frameworks

There is no binding international public legal framework governing the exchange of data between states. Hence, there is room for national, regional, and international initiatives.

National legislatures may pass laws that authorize collection of information for domestic immigration and security programs. For example, in the United States, Congress passed the Secure Travel and Counterterrorism Partnership Act of 2007, which requires travelers from Visa Waiver countries to register and receive travel authorization from the US Electronic System of Travel Authorization (ESTA) prior to their departure. Previously, the Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSVERA, H.R.3525) required all countries participating in the US Visa Waiver Program to incorporate biometric identifiers in their passports by October 2004, which was later extended to November 30, 2006.

European countries and the European Union have also passed legislation authorizing them to collect, retain, and process personal data for security and immigration purposes. On the national level, the UK e-Borders system, for example, "make[s] full use of the latest electronic technology to provide a way of collecting and analy[z]ing information on everyone who travels to or from the United Kingdom."[30] At the EU level, two major legal instruments allow governments to collect information on travelers. The first — the so-called Advance Passenger Information (API) directive of 2004 — aims to "improve border controls and combat […] illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities." [31] The second instrument — the regulation establishing the Visa Information System (VIS) — seeks to "improve the implementation of the common visa policy, consular cooperation, and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto".[32]

International Frameworks

Governments can also obtain authorization to collect and/or share information on travelers and other individuals through international, multilateral, regional, or bilateral agreements, such as the EU-US PNR Agreement, the EU-US Mutual Legal Assistance Treaty (MLAT), the Regional Movement Alert System (RMAS), the High-Value Data-Sharing Protocol to enhance asylum and other immigration-related fraud detection among the Five Country Conference, and the cooperative program with Interpol to

[30] Home Office, UK Border Agency, "e-Borders," http://www.bia.homeoffice.gov.uk/managingborders/technology/eborders/.

[31] Official Journal of the European Union, "Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communciate passenger data," August 6, 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32004L0082%3AEN%3AHTML.

[32] Not all EU Member States have implemented the API directive (though some of them had similar national instruments prior to the passage of the directive), and the European Commission is still setting up the Visa Information System. See: Official Journal of the European Union, "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)," August 13, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0060:0081:EN:PDF.

screen for lost and stolen passports.[33]

Most of these agreements originate from the interest and need among governments to find an international solution to reinforce national legislation that seeks to increase security measures against terrorism, transnational crime, and illegal immigration. The content of national legislation therefore can be extended internationally in its scope and reach. For those countries that have yet to pass national legislation on such mobility-security measures, signing an international agreement could potentially serve as a first step toward adopting such policies.

For example, the United States passed the Aviation and Transportation Security Act of 2001 (ATSA), the EBSVERA of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and amendments to the Tariff Act of 1930, which require private aircraft carriers and commercial airline and vessel companies to collect and submit certain information on all passenger and crew members who enter or leave the United States.[34] ATSA, for example, resulted in an interim final rule on June 25, 2002 that requires air carriers to make PNR information available to the Customs Service upon request.[35] The first EU-US PNR agreement signed in 2004 followed the passage of this national legislation.[36]

ATSA also mandated both foreign and domestic airlines flying to or from the United States to provide PNR data to US Customs and Border Protection (CBP). The three PNR agreements between the United States and the European Union since 2004[37] — the current version of which requires all air carriers operating passenger flights to the United States to submit PNR data stored in their reservation systems to DHS — were the source of much controversy and diplomatic tension.

From 2008, the United States, as part of its plan to expand the US Visa Waiver program (VWP), negotiated and reached bilateral agreements with several EU Member States on enhancing cooperation and combating serious crime. Among other things, the bilateral agreements allow the United States and its counterparts to access reference data in their respective automated fingerprint identification systems and, if permissible under their national laws, DNA profiles in their respective DNA analysis files.[38]

---

[33] For a list of programs implemented by DHS regarding the 9/11 Commission's Recommendations, see: US Department of Homeland Security, "Department of Homeland Security: Progress in Implementing 9/11 Commission Recommendations," July 22, 2009, http://www.dhs.gov/xlibrary/assets/dhs_5_year_progress_for_9_11_commission_report.pdf.

[34] Rail and bus carriers are not required to submit APIS data but can voluntarily provide similar information on their passengers and crew.

[35] The Customs Service was then under the US Treasury Department. With creation of the Department of Homeland Security, Customs functions now are carried out by DHS's US Customs and Border Protection division.

[36] US Government Printing Office, "Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States," Federal Register, June 25, 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-15935-filed.pdf.

[37] Official Journal of the European Union, "Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record data by air carriers to the United States Department of Homeland Security ,2007," August 4, 2007, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf.

[38] For an example of an agreement between the United States and another country on enhancing cooperation in preventing and combating serious crime, see: US Department of Homeland Security, "DHS and DOJ Sign Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime with the Republic of Estonia," September 29, 2008,

Several EU Member States signed an international agreement, the so-called Prüm Treaty of May 2005, to exchange DNA, fingerprints, and other personal data with each other, stepping up cross-border cooperation to counter terrorism and combat organized crime.[39] This treaty has served as a model for similar EU legal instruments as well as for the aforementioned transatlantic and bilateral agreements to enhance cooperation and combat serious crime. While the European Union itself does not have a PNR system like that of the United States, it has signed two other international agreements with Canada and Australia on exchanging and protecting PNR data.[40]

Regardless of whether governments adopt legislation that authorizes them to collect, process, and share information on travelers unilaterally, bilaterally, or internationally, the measures have a wide impact on people across the world. Even "unilateral" measures such as the US Advanced Passenger Information System (APIS) or the ESTA requirement for US Visa Waiver Program members affect large numbers of people. When government programs only affect foreigners, their adoption and implementation can cause diplomatic strain. However, bilateral or multilateral information-sharing agreements are just as, if not more, difficult to broker.

III. Major Concerns about Transatlantic Information Sharing

Given the wide range of movement that human mobility encompasses — from permanent immigration, humanitarian migration, business travel, tourism, criminal movement, and terrorist travel — governments have identified separating the *bona fide* travelers from those intending to inflict harm as one of their main challenges.[41] Despite a

---

http://www.dhs.gov/xnews/releases/pr_1222715330518.shtm. Most of the provisions of these agreements, especially those on the exchange of DNA and fingerprints, draw on the provisions of the Prüm Council Decision. See: Rocco Bellanova, "Prüm: A Model 'Prêt-à-Exporter'? The 2008 German-US Agreement on Data Exchange," (Brussels, Belgium: Center for European Policy Studies, 2009).

[39] Rocco Bellanova, "The 'Prüm Process': The Way Forward for Police Cooperation and Data Exchange?" in *Security vs. Justice? - Police and Judicial Cooperation in the European Union*, eds., Elspeth Guild and Florian Geyer (Farnham, United Kingdom: Ashgate, 2008), 203-221.

[40] A proposal for an EU-wide PNR system has been advanced since 2007, but the debates were politically frozen until full enactment of the Lisbon Treaty. The latest proposal for an EU PNR system can be found at Council of the European Union, *Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for law enforcement purposes* (Brussels, Belgium: April 17, 2009), http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf. The proposal has also raised several criticisms. See Evelien Brouwer, *Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights* (Study for the European Parliament, Brussels: European Parliament, 2009), http://www.statewatch.org/news/2009/jan/eu-pnr-ep-study.pdf.

[41] However, some have criticized the very idea of separating *bona fide* from *mala fide* travelers as the distinction could potentially lead to discrimination between the types and levels of information collected and shared based on the type of traveler. Some also argue that categorizing travelers in this way risks abandoning the principles of presuming innocence until proven guilty and due process for certain types of travelers. For example, in 2008 the European Data Protection Supervisor stated that, "The underlying assumption in the communications (especially in the entry/exit proposal) is worrying: all travelers are put under surveillance and are considered a priori as potential law breakers. For instance in the Registered Travelers system, only the travelers taking specific steps, through *ad hoc* registration and provision of detailed personal information, will be considered 'bona fide' travelers. The vast amount of travelers, who do not travel frequently enough to undergo such a registration, are thus, by implication, de facto in the 'mala fide' category of those suspected of intentions of overstay. This is contributing to an atmosphere of general distrust especially towards third-country nationals,

general understanding among North American and European countries that information sharing relating to human mobility is becoming one of the main tools in the fight against transnational crime and terrorism, the lack of transparency regarding how governments collect, filter, store, and disseminate personally identifiable information in practice has fueled concerns relating to privacy, data protection, and transparency.

In fact, while some see governments' need to collect information to weed out dangerous individuals as an inevitable reality, others deem it an invasion of privacy or connote the requirement to submit biometric information such as fingerprints while traveling with criminality. Most of the literature and political discourses have promoted finding the right balance between information collection and security as the best compromise to address these concerns. We believe that solutions can be found only by understanding and unpacking specific key issues at stake, especially the issues known in privacy and information security circles as proportionality, targeting, effectiveness, use and safeguarding of data, transparency, and accountability (including oversight and redress).

A well-functioning and effective transatlantic information-sharing regime should be fair, transparent, and uphold privacy standards that satisfy individuals' needs and rights, both in the United States and in the European Union. Given the importance of information sharing in catching terrorists and serious criminals when they attempt to cross international borders, the issue will remain high on the agendas of governments in North America and Europe in the years ahead.

A. Exchange and Processing of Personal Data by Governments: the Case of the EU-US PNR Agreement

Accessing, storing, processing, and exchanging personal data raise important questions relating to privacy and data protection. The adoption and implementation of information-sharing agreements raise sociopolitical, economic, and diplomatic issues, making privacy and data-protection issues controversial in legislative, policy, and expert circles.

Historically, the United States and some European countries have often passed privacy and data-protection laws as a result of public mistrust of government and corporations' handling of large amounts of private information. A series of scandals or cases of misconduct have fueled those concerns in the past, such as with the Watergate scandal in the United States or the proposal in France during the 1970s to create the SAFARI system, a centralized database interconnecting citizens' data. Both cases boosted support

---

while it remains to be proved how significantly it will help in fighting terrorism." See: European Data Protection Supervisor, "Preliminary Comments of the European Data Protection Supervisor on: - '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', COM(2008) 69 final; - Communication from the Commission to the European Parliament, the Council , the European Economic and Social Committee, and the Committee of the Region, 'Examining the creation of a European Border Surveillance System (EUROSUR),' COM(2008) 68 final; -Communication from the Commission to the European Parliament, the Council , the European Economic and Social Committee, and the Committee of the Region, 'Report on the evaluation and future development of the FRONTEX Agency,' COM(2008) 67 final," March 3, 2008, http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

to adopt laws limiting the government's ability to handle personal information.[42] Almost four decades later, the renewed interest, emphasis, and capability of governments to process personal data has revived debates on privacy legislation that have sometimes caused diplomatic disputes between the United States and the European Union. The agreement between the United States and the European Union that authorizes DHS to access and process PNR data for risk assessment, and potentially law enforcement and counterterrorism purposes — has become the most emblematic example of both the evolution of transatlantic security measures and the issues raised by such developments.[43]

The 2007 EU-US PNR agreement (see Appendix 1) is a transatlantic agreement between DHS and the European Council of Ministers that allows for and defines the collection and processing of PNR data for US-bound flights. Prior to a plane's departure from the European Union, DHS collects PNR data either by directly accessing the air carriers' databases (pull system) or by receiving information from them (push system).[44] Once DHS receives the information, it can identify potentially threatening passengers by running names against lists of known criminal suspects, known or suspected terrorists, and other databases and risk-profile patterns. Those identified are then subject to secondary checks.[45]

DHS had used PNR data for law enforcement purposes since 1992, but it was only after Congress adopted the Transportation and Security Act in 2001 that the systematic collection of PNR data became binding. Access to PNR data became a major transatlantic issue as it was perceived to be in conflict with EU data-protection legislation and, in particular, with the provisions of the EU Data Protection Directive regulating the transborder flow of information to third countries. As such, allowing the United States to access and process 'European' PNR data has generated criticism and sparked diplomatic and juridical debate.

A non-exhaustive list of such challenges include: criticism that the EU-US PNR agreement intrudes upon privacy and lacks transparency; inter-institutional legal battles over which government agencies are responsible for negotiating and implementing the agreement; transatlantic negotiations of three (partially) different agreements; a milestone judgment of the European Court of Justice on the scope and limits of the main European legal instruments on data protection; and a wide proliferation of similar information-sharing measures in other legal settings.[46.]

---

[42] In the United States, Congress adopted the Privacy Act in 1974 and France adopted its first privacy legislation, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, in 1978. For an overview of how the Fair Information Practice Principles have developed in the United States, see: Federal Trade Commission, "Fair Information Practice Principles," June 25, 2007, http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[43] In the United States, it is very important that administrative risk assessment or border screening is not used for law enforcement purposes because different privacy rules are applied for such activities (passengers are not considered suspects in the United States unless they are or become targets of a criminal investigation).

[44] The 2007 EU-US PNR agreement required DHS to switch to a push system by January 1, 2008 for air carriers that comply with DHS technical requirements. For those that have not complied with DHS technical requirements, the earlier pull system is used until the air carrier has a system that satisfies these requirements.

[45] See how US Customs and Border Protection uses ATS-P at: US Department of Homeland Security, "DHS/CBP-006- Automated Targeting System," August 6, 2007, http://www.dhs.gov/files/publications/gc_1185458955781.shtm#2.

[46] Official Journal of the European Union, "Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name

Perhaps most famously, Members of the European Parliament, EU data-protection authorities in the Article 29 Working Party (Art.29 WP), and civil-rights groups argued that the conclusion of the EU-US PNR agreements in 2004 and 2007 raised serious privacy concerns as they authorized DHS to share PNR data from airlines departing from the European Union with other US government agencies and third countries for security purposes if they met comparable EU privacy standards.[47]

The 2004 PNR dispute between the United States and the European Commission and the subsequent lawsuits filed by the European Parliament are examples of the challenges posed by the differing legal structures of the United States and the European Union. In 2006, the European Parliament successfully obtained an ECJ decision annulling the original 2004 EU-US PNR agreement.

The ECJ ruled that the PNR agreement and the determination by the European Commission that the pledges made by the US government to limit its use of PNR data in a number of ways[48] had been based on the wrong legal basis — namely that the agreement had been based in first pillar, which governs issues pertaining to the EC internal market, and not in the third pillar, which governs police and judicial cooperation in criminal matters (security issues). Given that the privacy protections guaranteed under the first and third pillars differ, the ECJ decision to annul the agreement made it imperative for the European Union to discuss data protection and privacy guarantees for sharing information for third pillar, or security and law enforcement-related, matters. Specifically, because the ECJ ruled that the EU-US PNR agreement should have been agreed as a third-pillar issue, the 1995 Data Protection Directive, which applies only to first-pillar issues, would not apply.[49]

Record data," March 21, 2006, http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_eng.pdf; Official Journal of the European Union, "Agreement between the European Union and Australia on the processing and transfer of European Union-source passenger name record (PNR) data by air carriers to the Australian customs service," August 8, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:213:0049:0057:EN:PDF; Commission of the European Communities, "Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes," November 6, 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en.

[47] The 1995 EU Directive on Data Protection mandated that third countries have comparable standards to the EU if EU Member States are to share information.

[48] For an explanation of the undertakings adopted by CBP in 2004, see Henriette Tielemans, Kristof Van Quathem, David Fagan, and Amalie Weber, "The Transfer of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision," in *BNA International: World Data Protection Report*, June 2006, http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf.

[49] Most notably, the European Union's pillar structure, created by the Maastricht Treaty in 1992, has been the source of confusion and legal and political debates on whether legislation relating to human movement should be adopted under the first pillar or the third pillar. While the European Union can make policies for issues that fall under the first pillar (they generally relate to the single market — the free movement of persons, goods, services, and capital among EU Member States, as well as cooperation among members on agriculture, the environment, competition, and trade), it normally cannot for issues that fall under the third pillar (they relate to Justice and Home Affairs issues such as police cooperation and criminal matters). In fact, countries do not transfer sovereignty over to the European Union with regard to second- and third-pillar issues and thus they must agree unanimously to adopt legislation falling under these two pillars. Legislation under the first pillar as it relates to human mobility covers policies such as the free movement of people within the Schengen Area, an EU-wide visa policy, and a common EU asylum policy. Human mobility-related legislation adopted under the

At the time of the decision, the European Data Protection Supervisor (EDPS), which has no US counterpart, issued an opinion that encouraged EU Member States to adopt a comprehensive legal instrument that would ensure the protection of personal data outside of the first pillar, which is covered by the 1995 Data Protection Directive.

Some European parliamentarians were outright opposed to a new agreement under the third pillar as it would decrease the oversight authority of the European Parliament, while others were open to one as long as it contained adequate safeguards.[50]

Given that the US privacy regime differs from that of the European Union and that airlines would be transmitting their own commercial data for border screening and risk assessment purposes, many Europeans viewed allowing DHS to receive PNR information as problematic.[51] When the Bush administration exempted the 2007 EU-US PNR agreement, the Arrival and Departure System (ADS), and the Automated Targeting System (ATS)[52] from the 1974 Privacy Act, it raised further privacy concerns among European citizens. These exemptions allowed the US government to not uphold privacy guarantees such as allowing it to collect information on how individuals exercise their right to assembly as well as an individual's race, ethnicity, religion, trade union membership, or political affiliation, and exempt itself from giving notice to those on whom it collects information and offering other adequate redress procedures.[53]

In January 2009, DHS announced that it would apply Privacy Act protections to foreigners who are neither US citizens nor US legal permanent residents.[54] Specifically in its privacy policy guidance, DHS states that "any personally identifiable information that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a US citizen, legal permanent resident, visitor, or noncitizen. Under this policy, DHS components will handle the personally identifiable information held in mixed systems for non-US persons in accordance with the fair information practices as set forth in the Privacy Act. Non-US persons have the right of

---

third pillar, which covers police and judicial cooperation in criminal matters involve policies relating to cooperation in organized crime, terrorism, trafficking in human beings, and other forms of crime.

[50] "ECJ puts end to EU air passenger data transfers to US," *The Euractiv Network*, May 31, 2006, http://www.euractiv.com/en/security/ecj-puts-eu-air-passenger-data-transfers-us/article-155680.

[51] Henriette Tielemans, Kristof Van Quathem, David Fagan, and Amalie Weber, "The Transfer of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision."

[52] ATS is a government system that maintains for 40 years secret and unreviewable terrorist risk profiles created based on data mining. These profiles determine whether individuals will undergo invasive searches of their persons or belongings. See "Automated Targeting System," Electronic Privacy Information Center, http://epic.org/privacy/travel/ats/.

[53] Edward Hasbrouck, James P. Harrison, John Gilmore, *Comments on DHS-2006-0060*, December 4, 2006, http://www.hasbrouck.org/IDP/IDP-ATS-comments.pdf; Electronic Privacy Information Center, *Comments of the Electronic Privacy Information Center to Department of Homeland Security on Docket Nos. DHS-2007-0042 and DHS-2007-0043 Notice of Privacy Act System of Records: US Customs and Border Protection, Automated Targeting System, System of Records and Notice of Proposed Rulemaking: Implementation of Exemptions: Automated Targeting System* (Washington, DC: Electronic Privacy Information Center, 2007), http://epic.org/privacy/travel/ats/epic_090507.pdf.

[54] US Department of Homeland Security, *Privacy Policy Guidance Memorandum – Memorandum Number: 2007-1 (As amended from January 19, 2007)* (Washington, DC: US Department of Homeland Security, 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf; US Department of Homeland Security, *Privacy and Civil Liberties Policy Guidance Memorandum – Memorandum Number: 2009-01* (Washington, DC: US Department of Homeland Security, 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

access to their personally identifiable information and the right to amend their records, absent an exemption under the Privacy Act; however, this policy does not extend or create a right of judicial review for non-US persons."[55]

The immediate future of the current EU-US PNR agreement is uncertain. The 2007 EU-US PNR agreement is in effect and requires airlines departing from all EU Member States to submit PNR data to DHS. But because not all EU Member States had ratified the agreement in their national legislatures before the Lisbon Treaty took effect, according to the terms of that treaty the agreement may be reconsidered under its new governmental arrangements.

The result is the current provisional application of the agreement. With the Lisbon Treaty now in force, the European Union no longer needs to await the ratification of the remaining Member States, but instead must receive consent from both the European Council and the European Parliament to conclude the 2007 EU-US PNR agreement. (Prior to the Lisbon Treaty, under the Treaty of Nice, the European Parliament only offered its opinion, not consent, for the PNR agreement.) In the case that either (but more likely the European Parliament) does not offer its consent to conclude an agreement, the European Union could be faced with provisionally suspending implementation of the EU-US PNR agreement.[56.]

B. Legal Framework Differences between the European Union and the United States

General

Public reception of data collection programs has been mixed. In 2008, Eurobarometer surveys found that on average only 28 percent of EU citizens were aware of the existence of national data-protection agencies in their countries and 82 percent agreed that, in the context of combating international terrorism, governments should be allowed to monitor personal details when individuals fly.[57] Eighty-four percent of data controllers in the EU-27 favored more harmonized rules on information sharing for security measures.[58]

At the same time, domestic privacy concerns about how governments collect information as well as the role of private companies in releasing information to public authorities are mounting. While most individuals do not understand the legal distinctions between and privacy implications of collecting, sharing, and processing information for intelligence, law enforcement, or private purposes, they are becoming increasingly aware that a significant amount of personal information circulates within government or private

---

[55] Ibid.
[56] "EU Parliament set to 're-open' visa deal with US," *The Euractiv Network,* October 6, 2009, http://www.euractiv.com/en/justice/eu-parliament-set-open-visa-deal-us/article-186093.
[57] Eurobarometer, "Data Protection in the European Union: Citizens' Perceptions," The Gallup Organization, February 2008, http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.
[58] The EU-27 is comprised of the following members of the European Union: Belgium, the Netherlands, Luxembourg, France, Germany, Italy, Denmark, Ireland, the United Kingdom, Greece, Portugal, Spain, Austria, Finland, Sweden, Cyprus, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia, Bulgaria, and Romania. Eurobarometer, "Data Protection in the European Union: Data Controllers' Perceptions," The Gallup Organization, February 2008, http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf.

databases.[59] The unease with how governments collect, store, share, and apply personal information to their programs and activities only grows when the data lands in the hands and jurisdictions of foreign governments.

Above all, while the United States and the European Union share most of the same data-protection principles (or "fair information practices"), there are significant differences in their privacy and data-protection regimes which have raised concerns about what information countries should agree to share with each other and how they should process that information. The United States and the European Union differ not only in their privacy and data-protection regimes, but also in the areas that are covered and exempted by these regimes.

International Guidelines on Privacy and Personal Data Protection

A number of international guidelines on sharing personal information among countries try to guide governments, businesses, and privacy advocates to design information-sharing frameworks that uphold privacy and personal data standards while facilitating information flows. The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 is one such example, as are the subsequent 1985 Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks.[60]

In 1990, the United Nations also adopted privacy guidelines concerning computerized personal data files that all UN Member States are responsible for implementing nationally. With regard to transborder data flows, the UN guidelines state that if two or more countries offer similar privacy protections, they should be able to share information freely as if it were circulating within a single country. If privacy safeguards diverge, states may require governments to enforce additional safeguards.[61]

Privacy and Personal Data Protection in the United States

In the United States, the 1974 Privacy Act governs privacy and data protection for the collection, maintenance, usage, and dissemination of personally identifiable information for security or law enforcement purposes.[62] The Privacy Act applies to information in a

---

[59] See for example James Risen and Eric Lichtblau, "E-mail Surveillance Renews Concerns in Congress," *The New York Times*, June 16, 2009, http://www.nytimes.com/2009/06/17/us/17nsa.html; Eric Lichtblau, "Telecoms Win Dismissal of Wiretap Suits," *The New York Times*, June 3, 2009, http://www.nytimes.com/2009/06/04/us/politics/04nsa.html?_r=1. In the summer of 2008, the French government attempted to pass two decrees establishing large databases storing information on citizens linked to public or political activities. The most known and debated was EDVIGE. See Meryem Marzouki, "ENDitorial: Massive Mobilization Against EDVIGE, The New French Database," *EDRI-gram*, July 16, 2008, www.edri.org/edrigram/number6.14/edvige-french-database.

[60] Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html; Organization for Economic Cooperation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html; Organization for Economic Cooperation and Development, "Cross-Border Privacy Law Enforcement," http://www.oecd.org/document/25/0,3343,en_2649_34255_37571993_1_1_1_1,00.html.

[61] European Commission, "United Nations guidelines concerning computerized personal data files," http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm.

[62] *The Privacy Act of 1974 (As Amended)*, Public Law 93-579, 93rd Cong., 2d sess. (December 31, 1974).

system of records, which contains personally identifiable information on individuals. While the Privacy Act, in a strictly legal sense, applies only to US citizens and lawful permanent residents, DHS amended its privacy policy in January 2009 to extend the application of the Privacy Act to systems of records that contain information on foreign visitors who are neither US citizens nor US legal permanent residents as well. This entitles foreign citizens to some but not all the rights of redress afforded to US citizens. Most importantly, foreign citizens still do not have a right of judicial review.[63]

In addition, the Privacy Act requires each government agency that maintains a system of record to publish a system of records notice (SORN) — a description of what it is and how it is used — in the *Federal Register*, the US government's official journal for publication of proposed new rules and regulations, final rules, changes to existing rules, and notices of meetings and adjudicatory proceedings (see Table 1 for a selection of SORNs maintained by DHS).[64]

While the Privacy Act contains rules for sharing information maintained in a system of records, each SORN also describes what information may be shared outside of the agency or department. For example, the SORN for APIS states when and how DHS may share information with any other federal, state, local, international, tribal, or foreign agency or multilateral governmental organization. Permissible circumstances include when DHS deems that sharing information with these entities would assist in enforcing civil or criminal laws, pursuing anti-terrorism efforts, collecting law enforcement intelligence, and helping to prevent exposure to or transmission of communicable or quarantinable diseases and combating other significant public-health threats.

The US system of data protection, as it is applied today, is not free from criticism. The automated targeting system (ATS) which the US government has used for screening purposes since the mid-1990s has greatly expanded and become increasingly automated since 2002. Privacy advocates argue that the government keeps millions of records on *bona fide* travelers in ATS but has no effective way to review information and correct errors. They further argue that some of the information collected by DHS violates the Privacy Act, which prohibits the US government from collecting information related to American's exercising of their First Amendment rights,[65] such as reading materials or people with whom they associate.[66]

The US Government Accountability Office (GAO) has raised several issues with how the federal government applies, or more aptly does not apply, the Privacy Act to the collection and use of personally identifiable information.[67] In particular, GAO

---

[63] US Department of Homeland Security, *Privacy Policy Guidance Memorandum – Memorandum Number: 2007-1(As amended fromJanuary 19, 2007)* (Washington, DC: US Department of Homeland Security, 2009), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[64] For a full list of DHS systems of records, see: US Department of Homeland Security, "Systems of Records Notice (SORNs)," October 14, 2009, http://www.dhs.gov/files/publications/gc_1185458955781.shtm#4.

[65] The First Amendment states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

[66] Matthew Harwood, "The Information DHS Stores on International Travelers," *Security Management*, September 10, 2009, http://www.securitymanagement.com/news/information-dhs-stores-international-travelers-006185.

[67] US Government Accountability Office, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information*, GAO-08-795T,

recommended that the US government:

- apply privacy protections consistently to all collection and use of personal information collected by federal agencies;[68]
- ensure that federal agencies limit their use of personally identifiable information to a stated purpose;[69] and
- establish effective mechanisms for informing the public about privacy protections, such as by creating a central privacy office or government web site dedicated to guaranteeing privacy at the federal level.[70]

---

http://www.gao.gov/new.items/d08795t.pdf; Senate Committee on Homeland Security and Governmental Affairs, "Lieberman, Collins Say Privacy Policy Needs to Catch Up To Digital Age," (press release, June 18, 2008), http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=38dce0aa-ab68-4478-9426-e5d9be649f01&Region_id=&Issue_id=baeab989-7f6a-4e7a-83b9-f18fa0a065c9.

[68] Currently, some collection and use of personally identifiable information are exempt from the Privacy Act. Specifically, if federal agencies do not retrieve information by a personal identifier, the Privacy Act's protections do not apply.

[69] The Fair Information Practices states that the use of personal information should be limited to a specified purpose. Current laws allow agencies to be vague in their public notices about how they will use information. Some experts recommend defining the limits of information use and requiring the government to establish a formal agreement with third countries before signing information-sharing agreements.

[70] Some experts recommend publishing system-of-records privacy notices that define the limitations on use and collection of personally identifiable data rather than in public notices in the *Federal Register*. They also recommend updating the Privacy Act to require the federal government to publish all notices on a standard website such as www.privacy.gov.

Table 1. Systems of Records Maintained by DHS Agencies

Department-wide

- DHS Freedom of Information Act (FOIA) and Privacy Act (PA) Record System
- DHS Redress and Response Records System
- DHS Complaint Tracking System
- Personal Identity Verification Management System (PIV MS)
- Civil Rights and Civil Liberties (CRCL) Matters

US Customs and Border Protection (CBP)

- Global Enrollment System (GOES)
- Advance Passenger Information System (APIS)
- Automated Targeting System (ATS)
- Border Crossing Information (BCI)
- Electronic System for Travel Authorization (ESTA)
- US Customs and Border Protection Treasury Enforcement Communication System (TECS)
- Nonimmigrant Information System (NIS)

US Immigration and Customs Enforcement (ICE)

- Student and Exchange Visitor Information System (SEVIS)
- Removable Alien Records System (RARS)
- Visa Security Program (VSP)
- Enforcement Operational Immigration Records (ENFORCE/IDENT)

Transportation Security Administration (TSA)

- Transportation Security Enforcement Record System
- Transportation Security Threat Assessment System
- Transportation Security Intelligence Service Files
- Transportation Worker Identification Credentialing System
- Registered Traveler
- Secure Flight Records

United States Visitor and Immigrant Status Indicator Technology (US-VISIT)

- Arrival and Departure Information System (ADIS)
- DHS Automated Biometric Identification System (IDENT)
- Technical Reconciliation Analysis Classification System (TRACS)

US Citizenship and Immigration Services (USCIS)

- Alien File (A-File) and Central Index System (CIS)
- Background Check Service
- Biometric Storage System
- Verification Information System
- Inter-Country Adoptions Security
- Fraud Detection and National Security Data System (FDNS DS)
- Benefits Information System
- Refugee Access Verification Unit
- Compliance Tracking and Monitoring System

Source: US Department of Homeland Security

Privacy and Personal Data Protection in the European Union

The protection of individual privacy and personal data in Europe is covered by two different rights, on privacy and data protection.[71] They do not have the same identical scope, even if they often overlap.

The right to privacy is based on the following international and EU legal instruments:

- Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR),[72] and the related case law of the European Court of Human Rights (ECtHR)
- Article 7 of the Charter of Fundamental Rights of the European Union[73]

The right of data protection is based on:

- Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the movement of such data (Data Protection Directive)[74]
- Directive 2002/58/EC on privacy and electronic communications[75]
- Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (Data Protection Framework Decision)[76]
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention 108)[77]
- Article 8 of the Charter of Fundamental Rights[78]

---

[71] Paul De Hert and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action," in *Reinventing Data Protection?* Eds., Serge Gutwirth et al. (Dordrecht, The Netherlands: Springer, 2009), 14-29.

[72] The Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms adopted in Rome on November 4, 1950, states in Article 8 (Right to respect for private and family life): "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[73] The Charter of Fundamental Rights of the European Union adopted in Strasbourg on December 12, 2007 states in Article 7 (Respect for private and family life): "Everyone has the right to respect for his or her private and family life, home, and communications."

[74] Official Journal of the European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," November 23, 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[75] Official Journal of the European Union, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector," July 31, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[76] Official Journal of the European Union, "Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters," December 30, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

[77] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS no. 108," January 28, 1981, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG.

[78] Article 8 (Protection of personal data) of the Charter of Fundamental Rights states: "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed

This framework is scattered and based on instruments with different legal natures and institutional settings. Three legal instruments are most important when it comes to examining the limits and shortcomings of privacy and data-protection laws in the context of security: the 1995 Data Protection Directive, the 1981 CoE Convention 108, and the 2008 Data Protection Framework Decision.[79]

Directive 95/46/EC, or the so-called Data Protection Directive, is the main piece of legislation governing data protection at the EU level. The objective of the Data Protection Directive is twofold: it seeks to protect "the fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data"[80] while ensuring the free flow of personal data. However, the directive does not apply to data processed for security or criminal law purposes.[81] The 2006 ECJ decision on the EU-US PNR agreement further curtailed the reach of the Data Protection Directive by prioritizing the final purpose of processing data over the very nature of data collection.[82] Data collected by firms but used for security purposes, the court held, are not covered by the Data Protection Directive. However, the Data Protection Framework decision of November 27, 2008, that will be discussed later, fills this void.

Notwithstanding such limitations, the 1995 Data Protection Directive remains a relevant reference point for the development of data protection in the field of Justice and Home Affairs, and in particular in the Area of Freedom, Security, and Justice (AFSJ) for at least three reasons: it covers AFSJ policies of the first pillar, such as those related to illegal immigration, visa, and asylum;[83] it created two of the main actors of data protection — the national data-protection authorities and the Article 29 Working Party;[84] and it still influences the definitions and principles of data-protection provisions of other legal instruments.

The CoE Convention 108 provides a legally binding enumeration of data-protection principles: data quality (including a range of principles from the fair and lawful collection

---

fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority".

[79] It is also important to underline that other *ad hoc* instruments contribute to AFSJ data protection, especially in the field of security, such as *ad hoc* data protection rules of AFSJ instruments; *ad hoc* data protection rules of EU or European agencies; *ad hoc* data protection rules of international agreement on data exchange between the EU and third countries; *ad hoc* data protection rules of the international agreement on data exchange between Europol and third countries; and national legislations.

[80] Article 1(1) of Directive 95/46/EC.

[81] This is stated in article 3(2) of Directive/95/46/EC.

[82] See Paragraphs 55-59 of Court of Justice of the European Union, "Joined Cases C-317/04 and C-318/04: European Parliament v Council of the European Union and Commission of the European Communities," May 30, 2006, http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=Rechercher$docrequire=alldocs&numaff=C-318/04&datefs=&datefe=&nomusuel=&domaine=&mots=&resmax=100.

[83] The Data Protection Directive covers the EURODAC database and will partially cover the Schengen Information System II (SISII) and Visa Information System (VIS) databases.

[84] On the establishment of independent data protection supervisor authorities, see Article 28 and Recitals 62 and 63; on the establishment of the Art.29 Working Party, cf. Articles 29 and 30 and Recitals 64 and 65. On the Art.29 Working Party competencies, tasks and powers, see: Gloria González Fuster and Pieter Paepe, "Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects," in *Security versus Justice?* Elspeth Guild and Florian Geyer, eds. (Farnham, United Kingdom: Ashgate, 2008), 131-132.

of data to purpose limitation and adequate, relevant, and not excessive collection; special categories of data; data security and data subjects' rights.[85]

Given the scope of the limitation of the Data Protection Directive, CoE Convention 108 was, and still is, the main reference in the fields of police and judicial cooperation. Several third-pillar instruments providing for *ad hoc* data-protection provisions use this convention as a threshold.[86] However, EU Member States are allowed to delay or not enforce the implementation of the convention's data-protection guarantees when they legally determine that government actions constitute "a necessary measure in a democratic society in the interest of: (a) protecting State security, public safety, the monetary interests of the State, or the suppression of criminal offences."[87] Finally, it is important to note that the convention was drafted prior to the widespread introduction of technologies that enable governments to profile and mine data, and serves as the backbone of most proposed security measures.[88]

Following three years of discussions and debates,[89] the Council of Ministers adopted the Data Protection Framework Decision (DPFD) on November 27, 2008 to offer a comprehensive EU framework for data protection in the field of police and judicial cooperation. The scope of the Framework Decision is limited to data shared among EU Member States and among Member States and authorities or information systems established on the basis of the Title VI of the Treaty on European Union (third-pillar security issues) or the Treaty establishing the European Community (first-pillar issues).

The DPFD excludes the sharing of domestic data among government agencies of a single Member State from its data-protection guarantees as well as data exchanged due to existing bilateral agreements with third States and EU third-pillar policies that already contain *ad hoc* data-protection provisions. Among the latter set are information-sharing laws pertaining to Europol, Eurojust, the Schengen Information System (SIS), the Customs Information Systems (CIS), as well as the Prüm Decision. The European Parliament and the European Data Protection Supervisor have criticized the limited scope of the DPFD,[90] arguing that it risks undermining the level of personal data

---

[85] These are stated in Articles 5, 6, 7, and 8 of the CoE Convention 108.

[86] For the EU PNR proposal, see Commission of the European Communities, "Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes," November 6, 2007, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en. For the Prüm Council Decision, see section C of this report.

[87] This is stated in Article 9 of the CoE Convention 108. The wording of Article 9 of Convention 108 echoes Article 8(2) of the ECHR.

[88] See Council of Europe, Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), *Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee (T-PD)*, March 13-14, 2008, http://www.statewatch.org/news/2008/aug/coe-profiling-paper.pdf.

[89] For an overview of the main debates and the main issues at stake, see Paul De Hert, Vagelis Papakonstantinou, and Cornelia Riehle, "Data protection in the third pillar: cautious pessimism," in *Crime, rights and the EU: The Future of Police and Judicial Cooperation*, ed. Maik Martin, (London: Justice, 2008), 121-194.

[90] European Parliament, "European Parliament legislative resolution of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters," September 23, 2008, http://www.statewatch.org/news/2008/sep/ep-resolution-dp-23-9-08.pdf; European Data Protection Supervisor, "EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step," November 28, 2008,

protection, allows for and even supports divergences in national data-protection standards, and adds complexity to an already complicated field.

Given the increased relevance of profiling techniques to travel-related information sharing agreements, the issue of "automated individual decisions"[91] and "processing of special categories of data"[92] are very sensitive and raise questions about whether or not the DPFD covers the sharing of such data. The DPFD permits "automated individual decisions" only if they are authorized by laws that also safeguard the data subjects' legitimate interests and allows governments to process sensitive data only if it is absolutely necessary and adequate safeguards are provided by national law. Like the EU Data Protection Directive, the DPFD also requires EU Member States to establish independent data-protection authorities and specify their powers.[93] Unlike the 1995 Data Protection Directive, however, it does not foresee the creation of a specific working group on data protection.

One of major weaknesses of the DPFD is that it allows for generous exemptions of data-protection principles concerning the "transfer to competent authorities in third States or to international bodies."[94] Specifically, the DPFD allows countries to derogate from the law in several cases, including important public interests and the provision of adequate safeguards from the receiving countries. All these criteria give governments ample room for interpretation, especially because the criteria on which they assess the level of adequacy remain quite vague.

Concerns Regarding the Differences in the EU and US Data-Protection Regimes

Definitions of "individual", and scope of judicial redress

Under the Privacy Act of 1974, individuals can request access to information pertaining to themselves in a system of records maintained by the US government.[95] However, given that an individual is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence,"[96] the issue of redress and the unavailability of civil remedies for noncitizens represent one of the major sticking points in the follow-up to discussions held by the EU-US HLCG. According to the definition of individual in the Privacy Act, EU citizens who are not US lawful permanent residents are excluded from

---

http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/08/11&format=HTML&aged=0&language=EN&guiLanguage=en.

[91] An automated individual decision is one that "produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject." See Article 7 of the Data Protection Framework Decision.

[92] Sensitive data include information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life.

[93] Namely: investigative powers (art.25(2)(a)); effective powers of intervention (art.25(2)(b)), and the power to engage in legal proceedings (art.25(2)(c)).

[94] See Article 13 of the Data Protection Framework Decision. The Framework Decision defines four criteria of transmitting information to third countries or international bodies: (1) it is linked to the principle of purpose limitation (namely that EU Member States share information to prevent, investigate, detect, or prosecute criminal offenses or to executive criminal penalties); (2) the recipient of the information is the one responsible for carrying out the actions stated in the previous point; (3) the Member State providing the information has offered its consent to transfer information; and (4) the third country or international body ensures an adequate level of data protection (art.13(1)).

[95] US Government Printing Office, "Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Records," *Federal Register*, Vol.73, No.223, November 18, 2008, http://edocket.access.gpo.gov/2008/E8-27205.htm.

[96] See § 552a (a)(2) of the 1974 Privacy Act.

the scope of the Privacy Act. In the European Union, however, the 1995 Data Protection Directive and the 2008 Data Protection Framework Decision cover all natural persons and are not limited to EU citizens and lawful permanent residents as privacy and data protection are considered human rights, as stated in EU human-rights law.[97]

The 1974 Privacy Act provision itself is a major obstacle in transatlantic negotiations to achieve a binding international agreement for sharing and protecting personal information.[98] Furthermore, the Privacy Act provisions on civil remedies are framed in a way that strongly limits the possibility of legal redress. To start a civil action against the agency, the behavior of the agency must have had an adverse effect on the individual (g)(1)(D). Moreover, the court must determine that the "agency acted in a manner which was intentional or willful" (g)(4). Such requirements, especially in a country that lacks a central independent privacy authority, can potentially limit a country's ability to enforce a legal redress system. Moreover, individuals will find it hard to prove that information sharing had an "adverse effect" on them, especially if they do not know if government technologies and information systems actually affected their ability to obtain a visa or enter a country.[99]

However, while the United States only offers judicial redress to US citizens and legal permanent residents for claims made under the US Privacy Act, it does offer all individuals regardless of citizenship access to redress through the Freedom of Information Act (FOIA).[100] In addition, US agencies have their own administrative redress procedures, such as the DHS Traveler Redress Inquiry Program (TRIP), under which all individuals, including non-US citizens, can seek redress.[101] For example, as stated in the APIS SORN, individuals seeking redress and/or contesting a record contained in APIS can either send a request to CBP, or to DHS TRIP. For instance, DHS permits individuals (including foreign nationals) to seek access to APIS data pertaining to them that carriers have provided to the US government.

According to a report by the DHS Office of Inspector General, TRIP does not positively affect the travel experiences of individuals seeking redress, only allows offices that are

[97] The purpose of the two instruments is inter alia to ensure a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy. Article 1(1) of the EU Data Protection Directive and Framework Decision (further explanation is given in the wording of Article 2(a), which is identical in both instruments) states that: "'personal data' mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."

[98] In its opinion on the adequacy level of the protection offered by the Privacy Act, the Belgian Data Protection Commission underlined the same points. See Commission de la Protection de la Vie Privée, "Objet: Examen du caractère adequate ou non du niveau de protection offert par le 'Privacy Act' américain de 1974, conformément à l'article 25 de la directive 95/46/CE," December 14, 1998, http://www.privacycommission.be/fr/docs/Commission/1998/avis_34_1998.pdf.

[99] Francesca Bignami, "European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining," *Boston College Law Review*, 48 (2007), 609-698.

[100] John Kropf, "Networked and Layered: Understanding the US Framework for Protecting Personally Identifiable Information," *World Data Protection Report*, The Bureau of National Affairs, 2007.

[101] Ibid.

thought to be the cause of redress to review the petition rather than allowing an independent review, and does not share information on redress case results.[102]

Oversight: Organizational or Structural Challenges
Organizational or structural differences between the United States and the European Union also pose challenges in discussing or negotiating information-sharing agreements. Differences in the institutional setups for privacy authorities in the United States and Europe often cause confusion and raise questions about how effective privacy oversight is on both sides of the Atlantic.

The European Union has multiple layers of independent data-protection authorities. First, all EU Member States are required to establish independent data-protection authorities under the EU Data Protection Directive. Some Member States, including France, Germany, and Spain, have also created subnational or regional data-protection authorities or antennae. Outside the common powers and competencies outlined in the Data Protection Directive and the Schengen Convention, national data-protection authorities vary by Member State in terms of their legal authority and human and economic resources.

As previously discussed, these national authorities established a standing Working Party called Art.29 WP, which has become one of the main pan-European actors in the field of privacy and data protection. Art.29 WP has the power to deliver opinions on the level of data protection both in the European Union and in third countries. While its scope is limited by the EU Data Protection Directive to issues pertaining to the first pillar, Art.29 WP has issued recommendations on all matters relating to the processing of personal data and created a Working Party on Police and Justice to monitor developments in the third pillar.

Finally, national data-protection authorities also send their officials to the Europol and Eurojust Joint Supervisory Bodies to oversee whether these two EU agencies effectively comply with their own data-protection frameworks.

In 2001,[103] the European Union established the European Data Protection Supervisor (EDPS), an EU institution tasked specifically with supervising, consulting, and cooperating with EU Member States on matters pertaining to privacy and data protection. EDPS is responsible for supervising the management of EURODAC and the future Visa Information System (VIS) and advising EU institutions on all matters relating to data processing and related proposals. Finally, it cooperates with other data-protections authorities on third-pillar issues.

The United States lacks a single, overarching, central privacy office. The US government has a variety of monitors that stem from its constitutional setup. These include, but are not limited to, the OMB Director, GAO, each federal department's Office of Inspector General (OIG), Chief Privacy Officers within federal agencies, a Civil Liberties

[102] US Department of Homeland Security, Office of Inspector General, *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (Redacted),* September 2009, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf.
[103] Official Journal of the European Union, "Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data," January 12, 2001, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf.

Protection Officer in the Office of the Director of National Intelligence, the five-member Privacy and Civil Liberties Oversight Board, as well as the Archivist and congressional committees. Federal agencies also publish SORNs and Privacy Impact Assessments (PIA) for their respective systems of records in addition to administrative processes that allow individual to seek redress, such as DHS's TRIP.[104] Furthermore, all individuals, regardless of nationality can request information regarding personal data through FOIA. These privacy players provide adequate protections in the processing of personally identifiable information.[105]

GAO, for example, is an arm of Congress that conducts investigations focusing on the processes that agencies use in their programs. Because inspectors general are part of their respective departments, many EU Member States often misperceive these offices as lacking true independence. Their reports and actions, however, provide evidence to the contrary, and they are indeed independent.[106] In addition to GAO and the inspectors general, DHS also has an independent Chief Privacy Officer with whom all agencies within the department work as they initiate new programs. Finally, congressional committees monitor and maintain oversight of government activities through hearings.

Some privacy advocates in the United States have criticized the setup of the US privacy regime.[107] One report found that two out of three US government agencies established after 9/11 and responsible for privacy policy — the DHS Privacy Office, the President's Civil Liberties and Privacy Oversight Board, and the Office of the Director of National Intelligence's Civil Liberties Protection Office — have taken either no or very limited actions that have had very little effect on privacy due to institutional problems or misinterpretation of their respective mandates, and that the DHS Privacy Office is the most active.

While privacy agencies within the US government can succeed in limiting executive choices, the fact that the DHS Chief Privacy Officer is a political appointee could potentially undermine the necessary oversight. Some experts describe EU data-protection authorities as more structurally independent than US privacy agencies.[108] Moreover, US privacy agencies in general lack powers to investigate and sanction privacy violations.

EU Data Protection Authorities (DPAs) also face challenges in limiting government powers to share personal information in the field of law enforcement and security. In

---

[104] However, according to David Sobel, Senior Counsel with the Electronic Frontier Foundation, DHS TRIP does not allow a traveler to challenge an agency decision in court because the Automated Target System is exempt from certain requirements under the 1974 Privacy Act including the right to "contest the content of the record." He says that a traveler has no ability to correct erroneous information. See Ellen Nakashima, "Collecting of Details on Travelers Documented: US Effort More Extensive Than Previously Known," *The Washington Post*, September 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/21/AR2007092102347_2.html.

[105] For a comprehensive discussion of US privacy actors, see John Kropf, "Networked and Layered: Understanding the US Framework for Protecting Personally Identifiable Information."

[106] For example, it was the State Department OIG that revealed the scandal involving a State Department employee who searched for passport information on the presidential candidates in 2008.

[107] Marc Rotenberg, "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11," (working paper, Social Science Research Network, September 2006), http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID933690_code678302.pdf?abstractid=933690&mirid=1.

[108] Francesca Bignami, "The US Privacy Act in Comparative Perspective," (Contribution to the European Parliament Public Seminar: "PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?" March 26, 2007).

fact, not all EU DPAs have the same powers to control government agencies and sanction them when in violation of national privacy and data-protection laws. Furthermore, as highlighted by a 2009 RAND report, they are often understaffed and lack resources.[109] This last problem is shared by US privacy offices and institutions charged with privacy oversight.[110] EU DPAs are authorized to lobby and play a key role in offering policy recommendations that add to the public debate on data protection and privacy. In the United States, GAO, civil-society groups, and corporate lobbies play the role of issuing recommendations to Congress.

Independent data-protection authorities are central to the fundamental right to data protection, as enshrined by Article 8 of the EU Charter of Fundamental Rights. This article prescribes that compliance with data-protection rules "shall be subject to control by an independent authority."

Data-protection authorities offer a potentially effective forum for mediating between individuals and governments in the context of security-related information sharing. However, the EU model of having independent data-protection authorities maintaining oversight over privacy and data-protection issues is but one model. The more integrated and layered structure of US oversight also presents advantages, especially when US privacy officers directly participate in transatlantic working groups that discuss and negotiate common principles and agreements. The inclusion of independent data-protection authorities in such groups not only allows them to be directly informed of the progress in negotiations and prospective cooperation, but also enables them to make important contributions to the debate, namely by introducing and suggesting potential privacy and data-protection safeguards during negotiations. The most important objectives on which both the Americans and Europeans agree are to have effective accountability, transparency, and remedy for information sharing among their governments.

While Article 8 of the EU Charter of Fundamental Rights requires an independent authority to monitor governments' compliance with data-protection rules, Article 13 of the 1950 European Convention on Human Rights requires states to guarantee the right to an "effective remedy."[111] As such, data-protection authorities on both sides of the Atlantic would at a minimum have to ensure that their respective oversight bodies have effective powers to remedy data-protection breaches. In the transatlantic context, whether or not such bodies have to be "independent" and what "independence" means remain open questions.

---

[109] Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri, *Review of the European Data Protection Directive*, (Santa Monica: Rand Corporation, 2009), http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf.

[110] Robert Gellman, "The American Approach to Privacy Supervision: Less than the Sum of its Parts," in *Challenges of Privacy and Data Protection Law*, eds. Maria Veronica Perez Asinari and Pablo Palazzi (Brussels, Belgium: Bruylant, 2008).

[111] According to Article 13 of the European Convention on Human Rights, "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

C. Transatlantic Decision-Making Forums

In addition to the different structural setups of privacy offices in the United States and the European Union, the two sides — DHS and the European Commission — have different competencies with regard to discussing or negotiating agreements. While DHS's mandate covers all JHA issues, the European Commission can only negotiate first-pillar aspects of JHA due to EU Member State prerogatives to discuss third-pillar issues pertaining to judicial and law enforcement cooperation. The European Union's legal-pillar structure makes it appropriate for EU Member States or the Council of the (JHA) Ministers, not the European Commission, to bilaterally discuss with the United States information-sharing agreements relating to travel and security.

The United States has several avenues to pursue internationally binding agreements. One is to sign a treaty, which, in the United States, means that the agreement must be made "by and with the Advice and Consent of the Senate" (Article II, Section 2, Clause 2 of the Constitution). In this case, the Senate may include reservations or conditions to the negotiated treaty or refuse to give its approval by choosing not to vote on the treaty or failing to pass it with a two-thirds majority. The EU-US Mutual Legal Assistance Treaty (MLAT), which came into force in November 2009, was passed under this treaty-making process.

The other is for the United States to sign an executive agreement, a form of internationally binding agreement made by the executive branch that is not submitted to the Senate for its advice and consent. For a number of reasons, the United States has increasingly concluded executive agreements with foreign governments, sometimes in the form of congressional or statutory agreements (agreements which Congress has previously authorized through domestic legislation) and others in the form of sole-executive or presidential agreements (which the president authorizes under his constitutional authority).

Executive agreements enter into force as soon as they are signed by both negotiating parties. Despite the Senate's relatively diminished role in executive agreements, the Case-Zablocki Act of 1972 requires all executive agreements be transmitted to Congress within 60 days of their entry into force, including those that are classified for security reasons. The EU-US PNR Agreement was passed under the executive agreement process.[112]

Some international agreements are nonbinding if they are only political agreements. Such agreements are not subject to congressional oversight or judicial scrutiny. However, parties that come to a political agreement may make a moral effort to be bound by the terms of the agreement and/or eventually find a way to make it legally binding. Given the lack of congressional oversight of such agreements, members of Congress may have to learn about their content and examine them through other forums. One possible forum for enhancing political discourse on legislation in the transatlantic context is the Transatlantic Legislators' Dialogue.[113]

---

[112] However, the original PNR regulation was passed in 2001 following 9/11. This served as the basis for PNR negotiations with third countries.

[113] European Parliament, Transatlantic Legislators' Dialogue, http://www.europarl.europa.eu/intcoop/tld/default_en.htm.

For the European Union, international agreements, such as the 2007 PNR agreement, are based on the structure set up in Article 24(1) of the Treaty on European Union, which states: "When it is necessary to conclude an agreement with one or more States or international organizations in implementation of this title, the Council may authorize the Presidency, assisted by the Commission as appropriate, to open negotiations to that effect. Such agreements shall be concluded by the Council on a recommendation from the Presidency." The European Parliament has no veto power over these agreements, and international agreements also largely escape ECJ oversight.

However, the European Union's decision-making structure concerning the negotiation and conclusion of international agreements are changing with the entry into force of the Lisbon Treaty. Under the Lisbon Treaty, the Council will remain the entity ultimately responsible for concluding negotiations, but the European Commission will play a stronger role in actually negotiating the agreements with foreign counterparts rather than merely assisting the Presidency in achieving its aims (art. 218(2-5) TFEU). The increased powers of the European Parliament are likely to have an important effect on how the European Union proceeds with its international information-sharing agreements.

Finally, it is particularly important to note that several security measures relying on data processing were initially discussed and sometimes adopted in different informal, and often private, forums that lacked transparency and accountability.[114] In the European Union, Member States have on many occasions initiated discussions on international agreements with their foreign counterparts, adopted measures outside of the EU legal framework, and then subsequently transposed them into that framework. This was the case with both the Schengen Agreement and the Prüm Treaty.

In the G6, an informal but structured group of officials of the interior ministries of France, Germany, Italy, Poland, Spain, and the United Kingdom, has met twice a year since 2003. G6 officials generally discuss topics that parallel those debated in the European Union, with issues such as cooperation on migration, law enforcement, and terrorism high on the agenda. Recently, the G6 has morphed into the G6 plus 1, ever since the United States was regularly invited to discuss transatlantic relations in these fields. The participation of the DHS Secretary at G6 plus 1 meetings reveals a trend that many discussions on privacy and data protection in the context of law enforcement occur on a bilateral or informal small-group basis.

Finally, following the 1995 G7 summit in Halifax, officials of the G7 — the grouping of seven industrialized economies (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States) — met to enhance cooperation on combating transnational crime. The Lyon Group, as the group was called, offered recommendations on how to enhance cooperation and established subgroups to address specific issues such as the legal basis for sharing information on criminals, immigration fraud, and human trafficking. The Lyon Group later transformed into the Roma/Lyon Group of

[114] United Kingdom House of Lords, European Union Committee, *Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamn*, July 11, 2006, http://www.statewatch.org/news/2006/jul/hol-behind-closed-doors.pdf; "G6-G8 Prum: Behind closed doors – policy-making in secret intergovernmental and international fora," *Statewatch*, http://www.statewatch.org/news/2006/sep/05eu-g6.htm; UK Home Office, "G6 Meeting (Berlin): Written answers and statements, 24 March 2009," *Statewatch*, March 24, 2009, http://www.statewatch.org/news/2009/sep/g6-meetings-hoc-answer.pdf; US Department of Homeland Security, "'G6 plus 1' Meeting in Germany," *Leadership Journal*, March 19, 2009, http://www.dhs.gov/journal/leadership/2009/03/g6-plus-1-meeting-in-germany.html.

the G8, which handles issues of counterterrorism, transnational organized crime, and biometric identity management to enhance security in travel and transportation.[115]

Transatlantic discussions on privacy and data protection also take place in working groups of experts and high-level officials. Such transatlantic high-level working groups began forming in the 1990s to discuss policies in a variety of areas but have increased their presence in the field of law enforcement since 2001.[116] HLCG, discussed below, is an example of such a group.

IV. Negotiating a Binding Legal Framework

Since 2006, the Troika process — when the Department of Justice (DOJ), DHS, and the European Commission meet twice a year to work out an agenda on cooperation on common issues — has made data sharing its primary focus during its meetings. The United States and the European Union were renegotiating a PNR agreement in 2006 when officials realized that any further productive negotiations on information sharing would require them to agree on a common set of principles on privacy and personal-data protection. At its November 2006 meeting, the group formed HLCG — an umbrella group to work on common data-privacy principles for sharing law enforcement information between the United States and the European Union.

HLCG was divided into two groups: the principals (senior policymakers) and the experts (involving law enforcement, data-privacy experts, and policy leadership). In the summer of 2008, HLCG agreed on a common set of principles, with some outstanding issues, which track the Fair Information Practice Principles — a set of principles, including 1) notice/awareness; choice/consent; 3) access/participation; 4) integrity/security; and 5) enforcement/redress, that the United States, Canada, and European countries have largely accepted since the 1970s as the underlying basis for national privacy and data-protection legislation.[117] In November 2009, HLCG resolved the outstanding issues and finalized a common set of principles. However, the informal nature of HLCG makes these principles nonbinding. The Council of Ministers made it clear that the European HLCG members were not acting on its behalf.[118]

Nevertheless, HLCG is a crucial forum that could provide a basis for establishing the necessary legal framework — a binding international agreement — for all information-sharing activities in matters pertaining to law enforcement and security between the United States and the European Union. The goal of reaching such an agreement would

---

[115] Group of 8, "G8 Declaration on Counter Terrorism," July 9, 2008, http://www.g8.utoronto.ca/summit/2009laquila/2009-counterterrorism.html.

[116] Patryk Pawlak, *Made in the USA? The Influence of the US on the EU's Data Protection Regime*," (Brussels, Belgium: Centre for European Policy Studies, 2009), http://www.ceps.eu/ceps/download/2680.

[117] The Fair Information Practices originated in the United States in 1973 when a government advisory committee became increasingly concerned about the use of private and public automated information systems that contained information on individuals. See: Robert Gellman, *Fair Information Practices: A Basic Guide*, November 10, 2009, http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

[118] US Department of Homeland Security, "EU-US Joint Statement on 'Enhancing transatlantic cooperation in the area of Justice, Freedom and Security,'" November 3, 2009, http://www.se2009.eu/polopoly_fs/1.21271!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf.

be twofold: (1) to enhance transatlantic cooperation in data and information sharing; and (2) to ensure data protection and privacy rights when doing so.[119] HLCG has identified a set of common principles, "acceptable as minimum standards when processing personal data for law enforcement purposes,"[120] as the best solution to achieve these twin objectives.

The HLCG Final Report lists 12 common principles of data protection and privacy for law enforcement purposes.[121] These principles are:

- Purpose Specification/Purpose Limitation
- Integrity/Data Quality
- Relevant and Necessary/Proportionality
- Information Security
- Special Categories of Personal Information (sensitive data)
- Accountability
- Independent and Effective Oversight
- Individual Access and Rectification
- Transparency and Notice
- Redress
- Automated Individual Decisions
- Restrictions on Onward Transfers to Third Countries

According to the Annex to the Final Report, HLCG members developed a common language for these principles. However, HLCG also introduced some caveats regarding this common language with regard to Principles 7 and 9.[122] Perhaps the most important HLCG remark concerns the redress principle. Even if both sides are in agreement that data subjects must have an effective means to seek redress, there are strong differences in the two legal systems concerning access to legal remedies. As previously discussed, the Privacy Act definition of individual excludes non US-citizens or aliens without a permanent residence permit. For the Europeans, the lack of judicial redress may undermine the credibility of any transatlantic agreement on privacy and data protection. For the United States, offering judicial redress would require updating the Privacy Act through new legislation.

---

[119] According to the HLCG Final Report, "The goal of the HLCG was to explore ways that would enable the EU and the US to work more closely and efficiently together in the exchange of law enforcement information while ensuring that the protection of personal data and privacy are guaranteed." See Council of the European Union, "Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection," May 28, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_intl_hlcg_report_02_07_08_en.pdf.

[120] Ibid.

[121] Council of the European Union, *Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection* (Brussels, Belgium: Council of the European Union, 2009), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/report_hlcg_info_sharingprivacydata_prot.pdf.

[122] In its report, HLCG notes that the principle of independent and effective oversight refers to their common goal rather than the need to implement the principle in the same way. The group notes that the principle of transparency and notice means that both the United States and the European Union should make information available to data subjects, but that the national laws will determine the modalities of information and their limitations.

The final report identified five other "outstanding issues pertinent to transatlantic relations":[123]

1. consistency in private entities' obligations during data transfers;
2. equivalent and reciprocal application of privacy and personal data-protection law;
3. preventing undue impact on relations with third countries;
4. specific agreements regulating information exchanges and privacy and personal data protection; and
5. issues related to the institutional framework of the European Union and the United States.[124]

In the fall of 2008, HLCG worked to find common wording for three of these five issues and agreed in spring 2009 on wording for another. The HLCG status report attached to the ministerial statement of December 16, 2008 offered some agreed text on most of the pending questions.[125] The text outlined how a prospective agreement would affect private actors and third countries, stating that they should not suffer any adverse impact as a result of diverging legal and regulatory requirements, and that HLCG would leave open the possibility of including in the scope of an agreement the collection and exchange of personal data with private actors.

The agreed text for the fourth outstanding issue (see above) suggested that a future general framework agreement could be complemented by more specific agreements relating to the processing of personal information in areas where the European Union and United States "agree that a clear legal necessity arises in particular due to a mutually recognized conflict of laws."[126]

By the beginning of October 2009, HLCG had yet to agree on the redress principle and on the fifth outstanding issue of specific agreements regulating information exchanges and privacy and personal-data protection. Officials from the US Departments of Justice, State, and Homeland Security, the EU Presidency, the European Commission, the European Data Protection Supervisor, the Europol Joint Supervisory Board, and several Member States met in Brussels on October 1, 2009 to increase mutual understanding of the EU and US legal frameworks that allow individuals to seek redress in the context of law enforcement. The experts agreed that while the US and EU redress mechanisms differed, both provided multiple effective procedures for administrative and judicial redress.[127]

The HLCG final report advances two main policy options for transferring their common principles into effective outputs: (1) the conclusion of a binding international agreement; or (2) a nonbinding instrument, such as "soft law" and/or a political declaration. HLCG members agreed that the first option is the best solution as it would achieve the twin

[123] Ibid.
[124] Ibid.
[125] The United States Mission to the European Union, "US, EU Issue Statement on Common Data Privacy and Protection Principles," December 12, 2008, http://useu.usmission.gov/Dossiers/Data_Privacy/Dec1208_SLCG_Statement.asp.
[126] Ibid.
[127] Council of the European Union, "Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection," November 23, 2009, http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf.

objectives of HLCG and provide the legal basis for more transatlantic agreements to exchange data and information in a mutually satisfactory way.[128]

However, this policy option would entail several new steps for the United States, especially if further national legislation is required. It would mean that the United States would have to amend its Privacy Act to extend redress rights to EU citizens. If this became the case, the Senate would become more active in drafting legislation or at the very least increase its oversight on international agreements that had previously been adopted as presidential executive agreements.[129] As for the second policy option, the recourse to soft law would offer less legal certainty and security.

The solution of the international binding agreement enjoys the declared support of most of the relevant actors. DHS Chief Privacy Officer Mary Ellen Callahan wrote in the department's leadership journal, "the next step is negotiating a binding international EU-US agreement based on these common principles to facilitate further cooperation while ensuring the availability of full protection for our citizens. The Department of Homeland Security looks forward to being a part of those efforts in the months ahead."[130]

In fact, even before the high-level political endorsement of this option in the November 3, 2009 EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom, and Security," several actors in the European Union, particularly the European Parliament, had expressed their preference for negotiating a binding international agreement.[131] In its resolution on the fight against terrorism, the Parliament "reaffirms the importance of cooperation with third countries in the prevention of and the fight against terrorism, and observes that the US is an essential partner in this field; considers that a common legal framework for police and judicial cooperation, with special emphasis on the protection of fundamental rights, especially of personal data, should be defined between the EU and the US, via an international agreement, ensuring appropriate democratic and parliamentary scrutiny at national and EU level."[132]

The EU Counter-Terrorism Coordinator, in his report to the Council of Ministers on the implementation of the EU counterterrorism strategy, stated that "it would seem that a legally binding EU-US agreement (to be negotiated on the basis of the Lisbon Treaty) would offer the best guarantees in terms of both data protection and a sustained

---

[128] Council of the European Union, "Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection," May 28, 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_intl_hlcg_report_02_07_08_en.pdf.

[129] Ibid.

[130] Mary Ellen Callahan, "US and EU Agree on Data Protection Principles," November 3, 2009, http://www.dhs.gov/journal/leadership/2009/11/us-and-eu-agree-on-data-protection.html.

[131] According to the EU-US Joint Statement on "Enhancing transatlantic cooperation in the area of Justice, Freedom and Security" of November 3, 2009, "We acknowledge the completion of the High Level Contact Group's more than two years of work to foster mutual understanding and identify a core set of common principles that unite our approaches to protecting personal data while processing and exchanging information for law enforcement purposes. We have important commonalities and a deeply rooted commitment to the protection of personal data and privacy albeit there are differences in our approaches. The negotiation of a binding international EU-US agreement should serve as a solid basis for our law enforcement authorities for even further enhanced cooperation, while ensuring the availability of full protection for our citizens."

[132] European Parliament, "European Parliament resolution of 12 December 2007 on the fight against terrorism," December 12, 2007, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0612&language=EN.

intensification of exchange of law enforcement data."[133]

Finally, in its opinion on the HLCG final report, the European Data Protection Supervisor underlined the complexities and the challenges linked to the protection of data exchanged and processed internationally for law enforcement purposes, but proposed the "development of a roadmap towards a possible [binding] agreement."[134] Currently, EDPS is also the only institution that has publicly offered possible guidelines and content for a binding international agreement.[135]

V. Moving Forward

Sharing information on individuals is now considered a vital government tool in combating transnational crime and terrorism. The discussions and debates on how the United States and the European Union will simultaneously share information on individuals and uphold mutually satisfactory privacy and personal data-protection standards are at a crossroads. In particular, three partially intertwined sets of challenges have emerged in the transatlantic experience.

First, the United States and the European Union have differed on what each views as the appropriate design for information-sharing measures in two major areas. First, the two sides differ on how they would like to integrate their respective agencies into the design and running of information-sharing measures. Second, they each have concerns about how to integrate federal and state actors in negotiations, and in the case of the European Union this means the players at the EU and Member State levels. Selecting the relevant agencies responsible for executing, overseeing, and updating information-sharing agreements is crucial in defining the purposes and proportionality of the measures as well as any relevant privacy and data-protection guarantees associated with such measures. The articulation of "federal" and "state" levels helps identify the number and nature of actors involved and in making negotiations more transparent. The question is how can the United States and the European Union resolve these differences in future negotiations?

The second set of challenges is linked to the first, and concerns the sociopolitical and legal contexts in which actors operate and frame information-sharing measures. First, rapidly changing technologies are enabling governments to handle larger amounts of information, but such changes in technological capacity are also making policymakers contemplate incorporating new types of information on individuals and innovative ways of collecting such data. Second, most of the actors involved, and especially executive agencies and interior ministries, perceive threats as continuously transforming, and thus require evolving approaches to tackle them. Such changes in technologies and security and law enforcement threats are further complicating an already vague legal framework

[133] Council of the European Union, "Implementation of the EU Counter-Terrorism Strategy – Priorities for further action," May 19, 2008, http://www.statewatch.org/news/2008/jun/eu-c-t-strategy-report-9417-08.pdf.
[134] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection," November 11, 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf.
[135] Ibid.

that is characterized by asymmetries between the United States and the European Union. Legal changes under the Lisbon Treaty make it an even greater challenge for the European Union to find sociopolitical and legal solutions to sharing information on individuals. If both sides only address some of the outstanding sociopolitical and legal challenges, they risk creating further fragmentation, political tension, and adequate information-sharing policy mechanisms. The key questions here are: what political triggers can the United States and the European Union use to induce the creation of or changes in privacy and data-protection laws where needed, and how can they find consensual solutions that allow them to address specific emerging needs or evolving security threats?

The third challenge is to solve pending US-EU information-sharing issues in an exemplary way. This means that the United States and the European Union should streamline information-sharing policies as they pertain to law enforcement and security to avoid the proliferation of *ad hoc* measures that rely on a variety of patchwork standards that do not relate to each other. Upholding fundamental rights and making costly measures efficient would help streamline such policies. The key is to maintain and apply a high standard for privacy and data protection while allowing for both sides to sign more specific agreements that meet the needs to respond to evolving security and law enforcement threats.

Here, we list eight key considerations for the United States and the European Union in working out a binding international agreement:

1) Policymakers should have a deep understanding of the roles and issues linked to the technology that enables governments and the private sector to share information. At the same time, no matter how advanced technologies are, officials should keep in mind that such technologies are not a silver bullet for overcoming their differences and potential obstacles in reaching a binding international agreement on sharing data for law enforcement purposes that satisfies their respective privacy and personal data-protection standards.

2) HLCG was an informal working group of senior policymakers and experts. While some experts have criticized the lack of clarity of other informal meetings of groups such as the Lyon Group and the G6 plus 1, the work of the HLCG has not been as secretive as that of other groups, and has not been directly criticized. The United States and the European Union should work toward negotiating a binding international agreement by publicizing the HLCG's work and deliberations. This will allow the public and legislators to gain confidence in a binding EU-US information sharing agreement. Further, the United States and the European Union should consider adding members to HLCG or the group that will likely succeed it. The United States should consider adding a senior representative who handles international privacy policy at the Department of State and the European Union should consider adding an EDPS official.[136]

3) While the United States and the European Union are working to establish a legal framework to share information for law enforcement purposes, their definition of

[136] HLCG has also experienced relatively success because of its inclusion of multiple actors and its general openness to discussing sensitive issues on a policy level that previously had only been discussed as technicalities. Broadening participation in the dialogue will help address technological changes and sociopolitical and legal issues in a more inclusive and scrutinized manner.

"law enforcement purposes" differ. The European Union defines law enforcement purposes as "use for the prevention, detection, investigation, or prosecution of any criminal offense,"[137] while the United States defines it as, "for the prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for noncriminal judicial or administrative proceedings related directly to such offenses or violations."[138] This issue is relevant to the extent that different definitions of "law enforcement" implicate different actors, agencies, processes, and types of information. By agreeing on what law enforcement means, both sides will be able to define who exactly should be involved in negotiations, what each of their government agencies needs, and where they should limit the sharing of information. It will also be important for US and EU policymakers to educate their publics and legislators about the different implications of their definitions for sharing information on individuals. In particular, they will need to negotiate how the wider definition adopted by the United States will be applied in practical terms and whether this will be acceptable to the Council of the European Union, the European Parliament, and the European public.

4) The United States and EU Member States have developed different approaches and laws pertaining to privacy and data protection and attribute different values to rights to privacy and data protection. However, they also share several principles on privacy and data protection and respect and uphold other democratic values such as the rule of law. The two sides should consider and learn more about the merits and disadvantages of their respective privacy regimes rather than focus on advocating one model over another. The European Union's setup of having multiple layers of independent data-protection authorities, both at the national and EU levels, and the US layered and networked approach to privacy each has its strengths and weaknesses.[139] That said, the United States needs to seriously consider implementing GAO recommendations, among others, to better guarantee privacy and data protection for personally identifiable information. This may mean establishing a central privacy office for the US federal government or creating a web site for a central privacy office.

5) With the enhanced decision-making role of the European Parliament following the entry into force of the Lisbon Treaty, the United States and the European Union should engage in more frequent and influential discussions over key policy issues concerning information sharing and the nexus between human mobility and security more generally. This would increase general oversight of information-sharing programs and agreements for law enforcement purposes and as a result increase public confidence in current and potential new agreements and programs. The Transatlantic Legislators' Dialogue is one possible forum for these discussions.

---

[137] Council of the European Union, "Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection," November 23, 2009, http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf.

[138] Ibid.

[139] However, it is important to note that the US federal government has been criticized for not consistently applying privacy protections on personally identifiable information across all federal agencies. See previous section of this paper on Privacy and Personal Data Protection in the United States and US Government Accountability Office, *Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information*, GAO-08-795T, (Washington, DC: US Government Accountability Office, 2008), http://www.gao.gov/new.items/d08795t.pdf.

6) Future negotiations will not be quick and easy, especially if they involve a larger number of actors from different government agencies and branches of government. While governments may be tempted to curtail a longer procedure by relying mainly on informal forums, such as the G6 plus 1, they should opt for more open and transparent options. Most of the outstanding issues require legislative changes that are much needed in an era characterized by increased human mobility. The United States and the European Union need to update their respective privacy and personal data-protection laws to have them apply effectively to current security needs. Such laws should also clearly define how they apply to foreigners (legal nonpermanent residents and noncitizens) and include fair procedures to seek redress. The EU-US MLAT, which enhances cooperation between the United States and the European Union on criminal matters, could serve as a partial model for future information-sharing agreements. The MLAT enables the United States and the European Union to share information, on a case-by-case approach, to counter terrorism and combat human trafficking, smuggling, and other forms of transnational crime. It organizes requests for assistance between the European Union and the United States that are transmitted between designated central authorities. Article 9 of the MLAT states that a government that is requested by another government to provide information cannot refuse to provide that information on grounds of data protection unless in exceptional cases.

   Article 8 of the MLAT allows mutual legal assistance to administrative authorities, meaning that it can be used as a basis for exchanging data for administrative purposes (such as PNR). However, in contrast to the EU-US PNR agreement, which allows for the transfer of data in bulk, the MLAT authorizes information exchanges on a case-by-case basis.[140] The MLAT therefore offers a good basis for negotiating agreements to share certain types of information, but not for concluding an overall binding EU-US legal framework for sharing all types of information for law enforcement purposes.

7) The relative effectiveness of information-sharing agreements, such as the EU-US PNR agreement, in stopping transnational criminals or terrorists from obtaining a visa, boarding a plane, or entering a country is unclear. The US and EU governments, through their respective government oversight offices or by publishing annual reports, should publicize the effectiveness of such programs and issue recommendations on how to make data collection and processing more efficient and effective. For example, policymakers should consider whether or not it is more effective to continue collecting, processing, and sharing bulk data as opposed to targeted and limited data on individuals. At the same time, they also need to focus on making criminal and terrorist watch lists more up-to-date and accurate.[141]

---

[140] However, there are also privacy concerns regarding the MLAT as it allows states to share information even if countries do not have the equivalent of specialized data-protection authorities or differ in the ways in which they protect personal data. Given the case-by-case approach, the MLAT is far -reaching and can bypass most of the sensitive issues of data protection (eg: the lack of data protection authority, the issue of redress). The MLAT therefore serve a good model for negotiating agreements to share certain types of information, but not for concluding an overall binding EU-US legal framework for sharing information. See Official Journal of the European Union, *Explanatory Note on the Agreement on Mutual Legal Assistance between the European Union and the United States of America* (Brussels, Belgium: Official Journal of the European Union, 2003).

[141] According to a report by the Office of Inspector General for the Federal Bureau of Investigations, 67 percent of cases reviewed by the OIG in which an FBI agent should have modified a watch list record failed to do so. Further, the FBI failed to remove 72 percent of the closed cases reviewed in a

8) The United States and the European Union should try to negotiate a binding international agreement that will serve as a reference for all future information-sharing agreements between them. A broad legal framework would allow both sides to maintain high standards for protecting fundamental rights and subsequently draft more specific agreements on sharing personal information that more accurately reflect and respond to the policies needed to act against evolving security threats.

The question of protecting personal information has ramifications beyond finding the right balance between security and privacy, or security and liberty. In the process of wrestling with these issues, powers, competencies, and relationships among government agencies and branches, individuals, and private companies will be affected. Acknowledging and resolving these major issues will allow the United States and the European Union to provide, as the European Parliament puts it, "[s]ecurity, [in support of freedom], […] pursued through the rule of law and subject to fundamental rights obligations."[142]

The evolving political and legal landscapes of the United States and the European Union, and in particular the election of President Obama and the entry into force of the Lisbon Treaty, raise questions about whether both sides will come to an agreement after complex negotiations, which require extensive legal analysis of security, law enforcement, intelligence, privacy, and personal-data protection. The work of HLCG, which began in 2006, lays important ground for negotiating a binding international agreement in the coming year. The challenge will be for negotiators on both sides of the Atlantic to learn about and reconcile their differences on privacy and personal data protection and implement the necessary changes on both the domestic and international fronts.

---

timely manner. See US Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices*, May 2009, http://www.justice.gov/oig/reports/FBI/a0925/final.pdf.

[142] European Parliament, European Parliament resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security, and justice serving the citizen – Stockholm programme, doc. P7_TA-PROV(2009)0090, Strasbourg, November 25, 2009, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009-0090+0+DOC+XML+V0//EN.

Appendix

Appendix I. Information-Sharing Agreements and Their Diplomatic Channels

Name:	EU-US Passenger Name Record (PNR) Agreement
Date(s)	First Agreement (2004), Second Interim Agreement (2006), Third Agreement (2007)
Objective	To prevent and combat terrorism and transnational crime effectively as a means of protecting their respective democratic societies and values.
Description	DHS receives PNR, which are stored in an air carrier's automated reservation/departure control systems, within 15 minutes of an aircraft's departure from the European Union and runs the data against watch lists.
Data Provider	All airlines departing from the European Union.
Data Receiver	US Department of Homeland Security, Customs and Border Protection.
Broad Description of Information Shared	Commercial airline reservation system data.
Specific Data Categories[143]	PNR record locator code Date of reservation/issue of ticket Date(s) of intended travel Name(s) Available frequent flier and benefit information (i.e., free tickets, upgrades, etc) Other names on PNR, including number of travelers on PNR All available contact information (including originator information) All available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction) Travel itinerary for specific PNR Travel agency/travel agent Code share (PNR) information Split/divided (PNR) information Travel status of passenger (including confirmations and check-in status) Ticketing information, including ticket number, one-way tickets, and Automated ticket fare quote All baggage information Seat information, including seat number General remarks including other services-related information (OSI), special services information (SSI), and special service requests (SSR) Any collected APIS information; and All historical changes to the PNR listed above.
Data Retention Period	Seven years as active files plus eight years in a dormant status. Exceptions for data actively used in law enforcement investigation: they are retained till the expiration of the procedure even if the formal retention period expires before.

[143] For a comparison between the prior 34 PNR data fields and the current 19, see "EU: European Commission to propose EU PNR travel surveillance system," *Statewatch*, July 15, 2007, http://www.statewatch.org/news/2007/jul/03eu-pnr.htm.

Name:	Advance Passenger Information System (APIS)
Date(s)	April 2005.
Objective	To perform counterterrorism and/or intelligence, law enforcement, and public security queries to identity risks to the aircraft or vessel, to its occupants, or to the United States and to reduce delays in the processing of arriving passengers at airports.
Description	DHS receives API within 15 minutes in advance of a passenger's and crewmember's arrival in or departure from the United States and runs the list against CBP's law enforcement databases, including information from the government's single consolidated Terrorist Screening Database (TSDB) and information on individuals with outstanding wants or warrants. DHS also receives from pilots an electronic Notice of Arrival and/or Departure no later than 60 minutes prior to departure from the United States or an airport overseas. After the pilot submits the eAPIS manifest to CBP, CBP determines whether the flight may arrive into or depart from the United States. CBP's response is transmitted to the pilot or his designee via email and the pilot should print the page to keep on the aircraft during the flight.
Data Provider	All private aircrafts[144] and commercial airlines and vessels.
Data Receiver	US Department of Homeland Security, Customs and Border Protection.
Broad Description of Information Shared	Passenger and crew manifests.
Specific Data Categories	Complete name Date of birth Gender Country of citizenship Passport/alien registration number and country of issuance Passport expiration date Country of residence Status on board the aircraft, vessel, or train Travel document type US destination address (for all private aircraft passengers and crew, and commercial air, rail, and vessel passengers except for US citizens, lawful permanent residents, crew, and those in transit) Place of birth and address of permanent residence (commercial flight crew only) Pilot certificate number and country of issuance (flight crew only, if applicable) PNR locator number. [The PNR locator number allows CBP to access PNR consistent with its regulatory authority under 19 CFR 122.49.d and the system of records notice for the Automated Targeting System, DHS/CBP-006, published August 6, 2007, 72 FR 43650.] *Commercial air and vessel carriers must also provide:* Airline carrier code Flight number Vessel name Vessel country of registry/flag International Maritime Organization number or other official number of the vessel Voyage number Date of arrival/departure

[144] A private aircraft is one, other than government or military, which is not engaged in carrying passengers or cargo for compensation. A commercial aircraft is one transporting passengers and/or cargo for some payment or other consideration, including money or services rendered.

	Foreign airport/port where the passengers and crew members began their air/sea transportation to the United States. *For commercial aviation passengers and crew members destined for the United States*: The location where the passenger and crew members will undergo customs and immigration clearance by CBP. *For commercial passengers and crew members who are transiting through (and crew on flights over flying) the United States and not clearing CBP*: Foreign airport/port of ultimate destination Status on board (whether an individual is crew or non-crew). *For commercial passengers and crew departing the United States*: The final foreign airport/port of arrival. *For pilots of a private aircraft*: Aircraft registration number Type of aircraft Call sign (if available) CBP issued decal number (if available) Place of last departure (ICAO airport code, when available) Date and time of aircraft arrival (or departure, for departure notice) Estimated time Location of crossing US border/coastline Name of intended airport of first landing Owner/lessee name (first, last, and middle, if available, or business entity name) Owner/lessee name (number and street, city, state, zip code, country, telephone number, fax number, and email address) Pilot/private aircraft pilot name (last, first, and middle, if available). Pilot license number Pilot street address (number and street, city, state, zip code, country, telephone number, fax number, and email address) Pilot license country of issuance Operator name (for individuals: last, first, and middle, if available, or name of business entity, if available) Operator street address (number and street, city, state, zip code, country, telephone number, fax number, and email address) Aircraft color(s) Complete itinerary (foreign airport landings within 24 hours prior to landing in the United States) 24-hour emergency point of contact (e.g. broker, dispatcher, repair shop, or other third party knowledgeable about this particular flight, etc), Emergency contact's name (first, last, and middle, if available) Emergency contact's telephone number (as applicable).
Data Retention Period	No more than 12 months from the date of collection. After 12 months, the APIS data are erased. However, certain APIS information is copied to the Border Crossing Information System (BCI), a subsystem of the Treasury Enforcement Communication System (TECS). APIS data for individuals who are subject to US-VISIT requirements (all visitors and lawful permanent residents) is also transferred to the Arrival and Departure Information System (ADIS) to allow DHS to track foreign nationals who overstay their visas. These APIS data include: Complete name Date of birth Gender Citizenship Country of residence

	Status on board the vessel US destination address Passport number Expiration date of passport Country of issuance (for nonimmigrants authorized to work) Alien registration number Port of entry Entry date Port of departure Departure date.

Name:	**Electronic System of Travel Authorization (ESTA)**
Date(s)	2009.
Objective	To automatically query terrorist and law enforcement databases to determine, in advance of departure, whether the applicant is eligible to travel to the United States under the US Visa Waiver Program (VWP) or whether the applicant poses a law enforcement or security threat.
Description	Applicants electronically submit personal information via an online application before traveling to the United States by air or sea. If there is a match, CBP will further vet the individual. If the applicant is cleared for visa waiver travel, he or she will receive an electronic ESTA confirmation. If the applicant is denied an ESTA, he or she is asked to obtain a visa from the State Department.
Data Provider	Nationals of VWP countries wishing to travel to the United States without a visa.
Data Receiver	US Department of Homeland Security, Customs and Border Protection.
Broad Description of Information Shared	The same personal information on an individual that had been required on the I-94W form.
Specific Data Categories[145]	Full Name (first, middle, and last) Date of birth Gender E-mail address Phone number Travel document type (e.g., passport), number, issuance date, expiration date, and issuing country Country of citizenship Date of crossing Airline and flight number City of embarkation Address while visiting the United States (number, street, city, state) Whether the individual has a communicable disease, physical or mental disorder, or is a drug abuser or addict Whether the individual has been arrested or convicted for a moral turpitude crime, drugs, or has been sentenced for a period longer than five years Whether the individual has engaged in espionage, sabotage, terrorism, or Nazi activity between 1933 and 1945 Whether the individual is seeking work in the United States Whether the individual has been excluded or deported, or attempted to obtain a visa or enter the United States by fraud or misrepresentation Whether the individual has ever detained, retained, or withheld custody of a child from a US citizen granted custody of the child

[145] For a comparison between the prior 34 PNR data fields and the current 19, see "EU: European Commission to propose EU PNR travel surveillance system," *Statewatch*, July 15, 2007, http://www.statewatch.org/news/2007/jul/03eu-pnr.htm.

	Whether the individual has ever been denied a US visa or entry into the United States, or had a visa cancelled. (If yes, when and where) Whether the individual has ever asserted immunity from prosecution Any change of address while in the United States ESTA tracking number.
Data Retention Period	Information stored in ESTA is active for 3 years and inactive for 12 years. An ESTA authorization generally expires and becomes inactive two years after the last submission or change in information by the applicant. If a traveler's passport is valid for less than two years from when the traveler was approved for ESTA, the information will expire when the passport expires. Information in ESTA is retained for one year after the ESTA expires. After this period, the inactive account information will be purged from online access and archived for 12 years. Data linked at any time during the 15-year retention period (3 years active, 12 years archived) to active law enforcement lookout records, CBP matches to enforcement activities, and/or investigations or cases, including applications for ESTA that are denied, will remain accessible for the life of the law enforcement activities to which they may become related. National Archives and Records Administration (NARA) guidelines for retention and archiving of data will apply to ESTA and CBP is in negotiation with NARA for approval of the ESTA data retention and archiving plan. The ESTA will over time replace the paper I-94W form. When an ESTA is used in lieu of a paper I-94W, the ESTA will be maintained in accordance with the retention schedule for I-94W, which is 75 years. (I-94W and I-94 data are maintained for 75 years to ensure that the information related to a particular admission to the United States is available for providing any applicable benefits related to immigration or other enforcement purposes.

Works Cited

Bellanova, Rocco. 2008. The 'Prüm Process': The Way Forward for Police Cooperation and Data Exchange? *Security vs. Justice? - Police and Judicial Cooperation in the European Union*, eds. Elspeth Guild and Florian Geyer. Farnham, United Kingdom: Ashgate.

Bellanova, Rocco. 2009. Prüm: A Model 'Prêt-à-Exporter'? The 2008 German-US Agreement on Data Exchange. Brussels, Belgium: Center for European Policy Studies.
Bignami, Francesca. 2007. European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining. *Boston College Law Review*, 48: 609-698.

Bignami, Francesca. 2007. The US Privacy Act in Comparative Perspective. Contribution to the European Parliament Public Seminar: "PNR/SWIFT/Safe Harbour: Are Transatlantic Data Protected?

Blanke, Jennifer and Thea Chiesa. 2009. *The Travel & Tourism Competitiveness Report 2009: Managing in a Time of Turbulence.* Geneva: World Economic Forum. http://www.weforum.org/pdf/ttcr09/ttcr09_fullreport.pdf.

Botting, Gary. 2005. *Extradition Between Canada and the United States.* Ardsley, NY: Transnational Publishers, Inc.

Brouwer, Evelien. 2009. *Towards a European PNR System? Questions on the Added Value and the Protection of Fundamental Rights.* Brussels: European Parliament, 2009. http://www.statewatch.org/news/2009/jan/eu-pnr-ep-study.pdf.

Callahan, Mary Ellen. 2009. US and EU Agree on Data Protection Principles. *Leadership Journal*, November 3, 2009. http://www.dhs.gov/journal/leadership/2009/11/us-and-eu-agree-on-data-protection.html.

Commission de la Protection de la Vie Privée. 1998. Objet: Examen du caractère adequate ou non du niveau de protection offert par le 'Privacy Act' américain de 1974, conformément à l'article 25 de la directive 95/46/CE. http://www.privacycommission.be/fr/docs/Commission/1998/avis_34_1998.pdf.

Commission of the European Communities. United Nations guidelines concerning computerized personal data files. http://ec.europa.eu/justice_home/fsj/privacy/instruments/un_en.htm.

_____. 2007. Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en.

_____. 2009. Report from the Commission to the European Parliament and to the Council: Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2008. http://www.statewatch.org//news/2009/sep/eu-com-ann-rep-eurodac-2008.pdf.

Council of Europe. 1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS no. 108. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG.

Council of Europe, Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). 2008. Application of Convention 108 to the profiling mechanism, Some ideas for the future work of the consultative committee (T-PD). http://www.statewatch.org/news/2008/aug/coe-profiling-paper.pdf.

Council of the European Union. 2008. Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection. http://www.dhs.gov/xlibrary/assets/privacy/privacy_intl_hlcg_report_02_07_08_en.pdf.

_____. 2008. Implementation of the EU Counter-Terrorism Strategy – Priorities for further action. http://www.statewatch.org/news/2008/jun/eu-c-t-strategy-report-9417-08.pdf.

_____. 2009. Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for law enforcement purposes. http://www.statewatch.org/news/2009/apr/eu-pnr-council-5618-rev1-09.pdf.

_____. 2009. Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection. http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf.

De Hert, Paul and Serge Gutwirth. 2009. Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action. *Reinventing Data Protection?* eds., Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwange, and Sjaak Nouwt. Dordrecht, The Netherlands: Springer.

De Hert, Paul, Vagelis Papakonstantinou, and Cornelia Riehle. 2008. Data protection in the third pillar: cautious pessimism. In *Crime, rights and the EU: The Future of Police and Judicial Cooperation*, ed. Maik Martin. London: Justice.

Electronic Privacy Information Center. 2007. "Automated Targeting System." http://epic.org/privacy/travel/ats/.

_____. 2007. Comments of the Electronic Privacy Information Center to Department of Homeland Security on Docket Nos. DHS-2007-0042 and DHS-2007-0043 Notice of Privacy Act System of Records: US Customs and Border Protection, Automated Targeting System, System of Records and Notice of Proposed Rulemaking: Implementation of Exemptions: Automated Targeting System. Washington, DC: Electronic Privacy Information Center. http://epic.org/privacy/travel/ats/epic_090507.pdf.

Euractiv. 2006. ECJ puts end to EU air passenger data transfers to US. May 31, 2006. http://www.euractiv.com/en/security/ecj-puts-eu-air-passenger-data-transfers-us/article-155680.

_____. 2009. EU Parliament set to 're-open' visa deal with US. October 6, 2009. http://www.euractiv.com/en/justice/eu-parliament-set-open-visa-deal-us/article-186093.

Eurobarometer. 2008. Data Protection in the European Union: Citizens' Perceptions. The Gallup Organization. http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.

_____. 2008. Data Protection in the European Union: Data Controllers' Perceptions. The Gallup Organization. http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf.

European Data Protection Supervisor. 2008. EDPS sees adoption of Data Protection Framework for police and judicial cooperation only as a first step. http://europa.eu/rapid/pressReleasesAction.do?reference=EDPS/08/11&format=HTML&aged=0&language=EN&guiLanguage=en.

_____. 2008. Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-11-11_High_Level_Contact_Group_EN.pdf.

_____. 2008. Preliminary Comments of the European Data Protection Supervisor on: - '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', COM(2008) 69 final; - Communication from the Commission to the European Parliament, the Council , the European Economic and Social Committee and the Committee of the Region, 'Examining the creation of a European Border Surveillance System (EUROSUR),' COM(2008) 68 final; -Communication from the Commission to the European Parliament, the Council , the European Economic and Social Committee and the Committee of the Region, 'Report on the evaluation and future development of the FRONTEX Agency,' COM(2008) 67 final. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

European Parliament. Transatlantic Legislators' Dialogue. http://www.europarl.europa.eu/intcoop/tld/default_en.htm.

_____. 2007. European Parliament resolution of 12 December 2007 on the fight against terrorism. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0612&language=EN.

_____. 2008. European Parliament legislative resolution of 23 September 2008 on the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. http://www.statewatch.org/news/2008/sep/ep-resolution-dp-23-9-08.pdf.

_____. 2009. European Parliament resolution of 25 November 2009 on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme, doc. P7_TA-PROV(2009)0090. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009-0090+0+DOC+XML+V0//EN.

Federal Trade Commission. 2007. Fair Information Practice Principles. http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

Fuster, Gloria González and Pieter Paepe. 2008. Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects. *Security versus Justice?* eds. Elspeth Guild and Florian Geyer. Farnham, United Kingdom: Ashgate.

Gellman, Robert. 2008. The American Approach to Privacy Supervision: Less than the Sum of its Parts. *Challenges of Privacy and Data Protection Law*, eds. Maria Veronica Perez Asinari and Pablo Palazzi. Brussels, Belgium: Bruylant.

Gellman, Robert. 2009. *Fair Information Practices: A Basic Guide.* http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

Group of 8. 2008. G8 Declaration on Counter Terrorism. http://www.g8.utoronto.ca/summit/2009laquila/2009-counterterrorism.html.

Hasbrouck, Edward, James P. Harrison, and John Gilmore. 2006. Comments on DHS-2006-0060. http://www.hasbrouck.org/IDP/IDP-ATS-comments.pdf

Harwood, Matthew. 2009. The Information DHS Stores on International Travelers. *Security Management*, September 10, 2009. http://www.securitymanagement.com/news/information-dhs-stores-international-travelers-006185.

Home Office, UK Border Agency. e-Borders. http://www.bia.homeoffice.gov.uk/managingborders/technology/eborders/.

Home Office, UK Border Agency. How we tested e-borders. http://www.ukba.homeoffice.gov.uk/managingborders/technology/eborders/testingeborders/.

Home Office, UK Border Agency. 2009. *Report of a Privacy Impact Assessment conducted by the UK Border Agency in relation to the High Value Data Sharing Protocol amongst the immigration authorities of the Five Country Conference.* http://www.bia.homeoffice.gov.uk/sitecontent/documents/managingourborders/strengthening/pia-data-sharing-fcc.pdf.

Hosein, Ian. 2004. The Sources of Laws: Policy Dynamics in a Digital and Terrorized World. *The Information Society* 20 (3): 187-199.

House of Lords, European Union Committee. 2006. *Behind Closed Doors: the meeting of the G6 Interior Ministers at Heiligendamn.*

http://www.statewatch.org/news/2006/jul/hol-behind-closed-doors.pdf.

House of Lords European Union Committee. 2008. *The Passenger Name Record (PNR) Framework Decision: Report with Evidence, 15th Report of Session 2007-08*. London, United Kingdom: The Stationary Office Limited.
http://www.statewatch.org/news/2008/jun/eu-pnr-uk-hol-report.pdf.

Interpol. A brief history of INTERPOL.
http://www.interpol.int/public/ICPO/Governance/SG/history.asp.

Kropf, John. 2007. Networked and Layered: Understanding the US Framework for Protecting Personally Identifiable Information. *World Data Protection Report*. The Bureau of National Affairs.

Lavenex, Sandra. 2005. Justice and Home Affairs. Towards a European Public Order? *Policy-Making in the European Union: Fifth Edition*, eds. Helen Wallace, William Wallace and Mark Pollack. Oxford, England: Oxford University Press.

Lichtblau, Eric. 2009. Telecoms Win Dismissal of Wiretap Suits. *The New York Times*, June 3, 2009.
http://www.nytimes.com/2009/06/04/us/politics/04nsa.html?_r=1.

Marzouki, Meryem. ENDitorial: Massive Mobilization Against EDVIGE, The New French Database. *EDRI-gram*, July 16, 2008.
www.edri.org/edrigram/number6.14/edvige-french-database.

Nakashima, Ellen. 2007. Collecting of Details on Travelers Documented: US Effort More Extensive Than Previously Known. *The Washington Post*, September 22, 2007.
http://www.washingtonpost.com/wp-dyn/content/article/2007/09/21/AR2007092102347_2.html.

National Commission on Terrorist Attacks Upon the United States. 2004. *9/11 and Terrorist Travel: Staff Report of the National Commission on Terrorist Attacks Upon the United States*.
http://www.9-11commission.gov/staff_statements/911_TerrTrav_Monograph.pdf.

Official Journal of the European Union. 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

_____. 2001. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf.

_____. 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

_____. 2003. Agreement on extradition between the European Union and the United States of America. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0027:0033:EN:PDF.

_____. 2003. Agreement on mutual legal assistance between the European Union and the United States of America. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:EN:PDF.

_____. 2003. Explanatory Note on the Agreement on Mutual Legal Assistance between the European Union and the United States of America.

_____. 2004. Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A32004L0082%3AEN%3AHTML.

_____. 2006. Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data. http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_eng.pdf.

_____. 2007. Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf.

_____. 2008. Agreement between the European Union and Australia on the processing and transfer of European Union-source passenger name record (PNR) data by air carriers to the Australian customs service. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:213:0049:0057:EN:PDF.

_____. 2008. Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:EN:PDF.

_____. 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). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0060:0081:EN:PDF.

Organization for Economic Cooperation and Development. Cross-Border Privacy Law Enforcement. http://www.oecd.org/document/25/0,3343,en_2649_34255_37571993_1_1_1_1,00.html.

_____. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html.

_____. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

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. http://www.ceps.eu/ceps/download/2680.

Risen, James and Eric Lichtblau. 2009. E-mail Surveillance Renews Concerns in Congress. *The New York Times*, June 16, 2009. http://www.nytimes.com/2009/06/17/us/17nsa.html.

Robinson, Neil, Hans Graux, Maarten Botterman, and Lorenzo Valeri. 2009. *Review of the European Data Protection Directive*. Santa Monica, CA: Rand Corporation. http://www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf.

Rotenberg, Marc. 2006. The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11. *Social Science Research Network*. http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID933690_code678302.pdf?abstractid=933690&mirid=1.

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 (1): 261-285.

Senate Committee on Homeland Security and Governmental Affairs. 2008. Lieberman, Collins Say Privacy Policy Needs to Catch Up To Digital Age. Press release, June 18, 2008. http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=38dce0aa-ab68-4478-9426-e5d9be649f01&Region_id=&Issue_id=baeab989-7f6a-4e7a-83b9-f18fa0a065c9.

Solove, Daniel J. 2008. Data Mining and the Security-Liberty Debate. *The University of Chicago Law Review* 75 (1): 343-362.

Steinbock, Daniel J. 2005. Data Matching, Data Mining, and Due Process. *Georgia Law Review* 40 (1), 1-86.

Statewatch. 2006. G6-G8 Prum: Behind closed doors – policy-making in secret intergovernmental and international fora.

http://www.statewatch.org/news/2006/sep/05eu-g6.htm.

_____. 2007. EU: European Commission to propose EU PNR travel surveillance system.
http://www.statewatch.org/news/2007/jul/03eu-pnr.htm.

The Privacy Act of 1974 (As Amended), Public Law 93-579, 93rd Cong., 2d sess. (December 31, 1974).

The United States Mission to the European Union. 2008. U.S., EU Issue Statement on Common Data Privacy and Protection Principles.
http://useu.usmission.gov/Dossiers/Data_Privacy/Dec1208_SLCG_Statement.asp.

Tielemans, Henriette, Kristof Van Quathem, David Fagan, and Amalie Weber. 2006. The Transfer of Airline Passenger Data to the US: An Analysis of the ECJ Decision. *BNA International: World Data Protection Report.*
http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf.

United Nations, Department of Economic and Social Affairs, Population Division. Trends in International Migrant Stock: The 2008 Revision.
http://www.un.org/esa/population/publications/migration/UN_MigStock_2008.pdf.

US Department of Homeland Security. 2007. DHS/CBP-006- Automated Targeting System.
http://www.dhs.gov/files/publications/gc_1185458955781.shtm#2.

_____. 2008. DHS and DOJ Sign Agreement on Enhancing Cooperation in Preventing and Combating Serious Crime with the Republic of Estonia.
http://www.dhs.gov/xnews/releases/pr_1222715330518.shtm.

_____. 2008. Homeland Security Presidential Directive 6: Directive on Integration and Use of Screening Information to Protect Against Terrorism.
http://www.dhs.gov/xabout/laws/gc_1214594853475.shtm.

_____. 2009. Department of Homeland Security: Progress in Implementing 9/11 Commission Recommendations.
http://www.dhs.gov/xlibrary/assets/dhs_5_year_progress_for_9_11_commission_report.pdf.

_____. 2009. EU-US Joint Statement on 'Enhancing transatlantic cooperation in the area of Justice, Freedom and Security.
http://www.se2009.eu/polopoly_fs/1.21271!menu/standard/file/EU-US%20Joint%20Statement%2028%20October%202009.pdf.

_____. 2009. "G6 plus 1" Meeting in Germany. In *Leadership Journal*, March 19, 2009.
http://www.dhs.gov/journal/leadership/2009/03/g6-plus-1-meeting-in-germany.html.

_____. 2009. Privacy and Civil Liberties Policy Guidance Memorandum – Memorandum Number: 2009-01. http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

_____. 2009. Privacy Policy Guidance Memorandum – Memorandum Number: 2007-1 (As amended from January 19, 2007). http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf;

_____. 2009. Systems of Records Notice (SORNs). http://www.dhs.gov/files/publications/gc_1185458955781.shtm#4.

US Department of Homeland Security, Customs and Border Protection. 2009. Global Entry with Expedited Entry into the Netherlands. http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/global_entry_flux.xml.

US Department of Homeland Security, Office of Inspector General. 2009. *Effectiveness of the Department of Homeland Security Traveler Redress Inquiry Program (Redacted).* http://www.dhs.gov/xoig/assets/mgmtrpts/OIG-09-103r_Sep09.pdf.

US Department of Justice. 2009. Attorney General Holder Speaks at EU/US Justice and Home Affairs Ministerial Meeting. http://www.justice.gov/ag/speeches/2009/ag-speech-091028.html.

US Department of Justice, Office of the Inspector General. 2009. *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Practices.* http://www.justice.gov/oig/reports/FBI/a0925/final.pdf.

US Government Accountability Office. 2008. Congress Should Consider Alternatives for Strengthening Protection of Personally Identifiable Information, GAO-08-795T. http://www.gao.gov/new.items/d08795t.pdf.

US Government Printing Office. 2002. Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or From the United States. *Federal Register.* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-15935-filed.pdf.

_____. 2008. Privacy Act of 1974; Customs and Border Protection Advanced Passenger Information System Systems of Records. *Federal Register*, 73 (223). http://edocket.access.gpo.gov/2008/E8-27205.htm.

About the Authors

Hiroyuki Tanaka
Hiroyuki Tanaka is a Research Assistant in the International, Mobility and Security, and Migration and Development programs at the Migration Policy Institute, where he focuses on highly skilled immigration in Europe, North America, and Asia and on mobility-related security issues.

Mr. Tanaka interned as a Guggenheim Intern and Oscar S. Straus Fellow at the Vera Institute of Justice, where he researched language access programs around the world and immigrant-police relations in the United States. As an undergraduate fellow of the Policy Research Institute for the Region, he organized events that addressed key policy issues affecting disadvantaged youth in the New York-New Jersey-Pennsylvania region. Mr. Tanaka holds a BA with honors from Princeton University, where he majored in the Woodrow Wilson School of Public and International Affairs and earned certificates in European Politics and Society and French. He also studied at the Institut d'Etudes Politiques in Paris as a member of a task force on immigration policy in Europe.

Rocco Bellanova
Rocco Bellanova researches data protection applied to security measures at the Facultés universitaires Saint-Louis (FUSL) and the Vrije Universiteit Brussel. He is member of the interdisciplinary Research Group on Law, Science, Technology, and Society and of the Centre de Recherche en Science Politique.

At FUSL, he also works as an assistant in international relations, political science, and contemporary political issues. His research interests are European and transatlantic security policies based on data processing, data protection and fundamental rights, and the development of the European Area of Freedom, Security, and Justice.

Susan Ginsburg
Susan Ginsburg is Nonresident Fellow at the Migration Policy Institute, where she headed the Mobility and Security Program. She is a member of the Department of Homeland Security's Quadrennial Review Advisory Committee and served on the Secure Borders and Open Doors Advisory Committee established by Secretary of State Condoleezza Rice and Homeland Security Secretary Michael Chertoff. Prior to joining MPI, she served as Senior Counsel and Team Leader on the staff of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), where she was responsible for research and policy recommendations concerning the entry of the 9/11 hijackers, terrorist travel, and border controls. She followed her work on the 9/11 Commission with consulting and policy writing focused on terrorist mobility.

Ms. Ginsburg previously worked as a consultant to nonprofit and academic institutions, providing strategic and operational planning relating to firearms policy. Prior to that, she worked at the Treasury Department as Senior Advisor and Firearms Policy Coordinator, Under Secretary for Enforcement. Before that, she was Chief of Staff to the Under Secretary for Enforcement (then overseeing the US Customs Service, the Secret Service, ATF, FLETC, FinCEN, and OFAC) and previously served as an attorney specializing in civil litigation.

Paul De Hert
Paul De Hert is an international human-rights expert, specializing in criminal law and technology and privacy law. At Vrije Universiteit Brussel, he holds the chair 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 core member of the internationally accepted 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*.