International Cooperation on Electronic Advanced Passenger Information Transfer and Passport Biometrics

Rey Koslowski

Woodrow Wilson International Center for Scholars and Rutgers University-Newark

Abstract:
This paper examines the development of US and EU border control capabilities and agendas in the wake of the September 11, 2001 attacks and international cooperation on international travel, migration and border control to increase security against future terrorist attacks. New US aviation security and border security legislation requires commercial airlines and ships to electronically submit passenger name record (PNR) data and passenger manifests before arrival to the US in order to pick out potential terrorists from growing flows of travelers. Border and visa security legislation also requires that all that visitors and migrants coming to the US carry travel documents containing biometric information and conditions countries' participation in the US Visa Waiver Program (most EU member states) on the issuance of machine-readable, tamper-resistant passports containing biometric data. The paper addresses diplomatic and political challenges inherent in data submission requirements that conflict with EU personal data protection norms as well as the challenges posed by diplomatic reciprocity, privacy protection and domestic political dynamics to the collection and exchange of biometric data.

Prepared for presentation at the International Studies Association Meeting, Montreal, March 17-20, 2004.

Acknowledgements: The research for this paper was supported by a fellowship from the Woodrow Wilson International Center for Scholars and a grant from the National Science Foundation Digital Government Program

DRAFT: Comments and suggestions welcome

Contact info:
Rey Koslowski
Fellow
Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Ave. NW
Washington, DC 20004-3027
Tel: 202-691-4066
Fax: 202-691-4001
E-mail: koslowskirj@wwic.si.edu
Web: http://www.wilsoncenter.org/index.cfm?fuseaction=sf.profile&person_id=34921

Introduction

The September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon starkly revealed the security vulnerabilities inherent in globalization as the hijackers entered the United Sates among the millions of migrants and visitors coming to the US on tourist and student visas. In response to the attacks, the United States, the European Union and its member states enacted policies to tightened border controls and devoted increasing budgets, staffing and technological resources to enforce those polices. Such increasing state capacity augurs against arguments maintaining that globalization is undermining state sovereignty

It has become clear, however, that no matter how many resources a state may throw at its borders, effective border controls that do not choke off international trade and legitimate travel require a high degree of international cooperation (see Flynn 2000). As US and EU border control officials took steps to tighten border controls through deploying new technologies in the effort to screen out threats from legitimate travel flows, border control officials on both sides of the Atlantic realized that transnational threats posed by terrorist networks required stepped-up international cooperation. While the split between the US and individual EU member states, such as France and Germany, over the Iraq war led some commentators to declare US-European relations as being in crisis, France and Germany, among other EU member states, were busily signing agreements and exchanging information with US border control authorities. US and EU member states may be increasing their state capacities to control borders but at the same time the European Commission and the US Department of Homeland Security have been taking international cooperation into sensitive areas of state sovereignty dealing with border controls, government surveillance, data collection and exchange that before September 11, 2001 would have been unthinkable. Nevertheless, there still are many legal and political obstacles to further

transatlantic cooperation in this area that have yet to be overcome. The solution set to overcoming these obstacles, ironically, points to even deeper and broader international cooperation in order to secure state borders.

This paper elaborates on this argument by examining the US and EU responses to the attacks of September 11th in the area of border security, the reverberations of US homeland security policy initiatives in Europe and the progress (or lack thereof) in international cooperation with respect to border and transportation security measures regulating travel between the US and the EU. The paper will first describe the post-September 11th US government reorganization to form a Department of Homeland Security while focusing on the US institutional frameworks and policy initiatives dedicated to increasing border and transportation security. Second, the paper places US initiatives in comparative perspective by reviewing European integration of border control policy and demonstrates that the EU and several of its key member states also reacted to Sept. 11 with major border control initiatives independent of US actions. The paper then turns to transatlantic cooperation in two areas: electronic submission of advanced passenger information, addressed in the third section, and a fourth section devoted to the issue of biometric passports as a requirement for future visa-free travel between the US and EU member states.

Border Security in the US

In the wake of the Sept. 11th attacks, the Bush Administration quickly established the Office of Homeland Security within the White House under the leadership of Tom Ridge so as to coordinate the anti-terrorism and border control efforts of key agencies spread across several cabinet-level departments of the federal government. At the time, the Bush administration opted

against a complete reorganization of government along the lines envisioned in the Hart-Rudman Commission (2001) report – a merger of the Coast Guard, US Customs Service and the US Border Patrol (a part of the Immigration and Naturalization Service (INS) into the Federal Emergency Management Agency to form a new Department of National Homeland Security. Senator Joseph Lieberman led Democrats in the Congress on the issue by proposing such a merger in an October 2001 draft bill but six months later in early April 2001 he lamented that there had been little progress toward such administrative restructuring (Lieberman 2002). Although there had been extensive consideration and discussion of border control agency administrative reform, the action of the Bush Administration appeared to be limited to reforming the INS by separating its enforcement functions from service functions (INS 2002). Homeland Security Director Tom Ridge then supported a plan to combine the law enforcement arm of the INS with the Customs Service in late April 2002 (Hillman 2002). Unbeknownst to the top managers in the INS and Customs Service who were preparing plans for the INS reorganization at the time, a small group within the White House was working on a government reorganization that went beyond what the Hart-Rudman Commission recommended.

On June 6, 2002, President Bush proposed the establishment of a new Department of Homeland Security (DHS) and the subsequent Homeland Security Act of 2002 merged 22 previously separate agencies into the new department's four "directorates" and three "elements" on March 1, 2003. The Border and Transportation Security (BTS) Directorate provides executive direction oversight, coordination and policy guidance to US Customs and Border Protection (CBP), US Immigration and Customs Enforcement (ICE), the Transportation and Security Administration (TSA), the Federal Law Enforcement Training Center (FLETC). The BTS Directorate also oversees the United States Visitor and Immigrant Status Indicator

Technology (US-VISIT) program, which is the entry-exist tracking system that collects digital photograph and fingerprint scan biometrics from those individuals traveling on a visa to the United States then runs watch list checks on the data collected. Given its mission, US-VISIT spans agencies of the BTS directorate, other DHS agencies as well as non-DHS agencies, such as the consular services of the US State Department. The "legacy" INS was divided up with the US Border Patrol and immigration inspectors going to US Customs and Border Protection, immigration investigators and detention services going to Immigration and Customs Enforcement (ICE) and the remainder forming US Citizenship and Immigration Services (USCIS). USCIS became one of the three "elements" along with the Coast Guard and Secret Service, whose directors all report to the Deputy Secretary of Homeland Security. The Department of Homeland Security Budget has increased from $31.2 billion in FY 2003, to $35.7 billion in FY 2004 and $37.6 billion in FY 2005 (DHS 2004: 3, 12).[1]

The parts of the DHS that are most relevant to transatlantic relations are Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). TSA is also involved in screening airline passengers from Europe and US Citizenship and Immigration Services (USCIS) administers non-immigrant and immigrant visas that EU nationals may hold. The US-VISIT program will become more relevant to US-EU relations as states that are not in the US Visa Waiver program join the EU in May 2004 and in the event that other EU member states are unable to remain in the program and be required to be enrolled in US-VISIT, photographed and provide fingerprint scans upon entry into the US.

To some extent prodded by Congressional critics who questioned the efficacy of a new department without a clear mission, in July 2002 the Bush Administration issued a "National

[1] These figures do not include funding for Project Bioshield, the government program to pre-purchase vaccines and medicines, which is authorized by separate legislation, nor does it include the funds from the 2004 Iraq supplemental appropriation.

Strategy for Homeland Security." The section on border and transportation security includes a box labeled "National Vision" and it states: "A single entity in the Department of Homeland Security will manage who and what enters our homeland in order to prevent the entry of terrorists and the instruments of terror while facilitating the legal flow of people, goods, and services on which our economy depends. The Department and its partners will conduct border security functions abroad to the extent allowed by technology and international agreements. (White House 2002a)." To realize this vision, the Bush administration had announced an initiative to create the "Smart Border of the Future." According to a White House statement: "The border of the future must integrate actions abroad to screen goods and people prior to their arrival in sovereign US territory, and inspections at the border and measures within the United States to ensure compliance with entry and import permits..… Agreements with our neighbors, major trading partners, and private industry will allow extensive pre-screening of low-risk traffic, thereby allowing limited assets to focus attention on high-risk traffic. The use of advanced technology to track the movement of cargo and the entry and exit of individuals is essential to the task of managing the movement of hundreds of millions of individuals, conveyances, and vehicles (White House 2002b)." In a dramatic illustration of the Administration's agenda, Richard Falkenrath, Deputy Assistant to the President and Deputy Homeland Security Advisor, drew an analogy likening the revolution in military affairs of the 1990s to the "revolution in border security" that is taking place now.[2]

The establishment of the new Department of Homeland Security is the largest reorganization of the federal government since the post-war formation of the Department of

[2] Response to author's question at "Transatlantic Homeland Security? European Approaches to "Total Defense," "Societal Security"and their Implications for the U.S." Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies Johns Hopkins University, Feb. 19, 2004.

Defense. Contrary to the impressions of some foreign observers,[3] the DHS and its border security measures are not just Bush Administration initiatives that will be dismantled should President Bush not be re-elected. As mentioned above, legislation enabling the formation of the DHS was first introduced and championed by Congressional Democrats and border security measures, including the aggressive deployment of information technologies were, in many cases, co-sponsored by Democrats and received broad bi-partisan support. Moreover, should the presumptive Democratic nominee, John Kerry, be elected to the Presidency, one could expect more, not less, spending by the Department of Homeland Security (Kerry 2004).

Border Security in the EU

There is no exact EU or EU member state counterpart to the US Department of Homeland Security. The new Department of Homeland Security is much closer in organization to European interior ministries that implement most border control functions than the previous dispersal of border control functions across the US federal government. Collectively, the border control divisions of EU member state interior ministries, however, are much larger than their US equivalent, the Bureau of Customs and Border Protection (CBP), despite staffing increases along the US southern border with Mexico during the 1990s and post-Sept. 11 hiring increases. The CBP has approximately 41,000 employees (DHS 2004: 19), which is only slightly larger than Germany's *Bundesgrenzschutz* (Federal Border Police) of 40,000 employees.[4] While the CBP includes Customs inspectors, if the number of German Customs inspectors were added into the

[3] Comments to the author during Q&A with American Studies scholars in China and Mexico after authors' presentations: "Homeland Security at What Cost?" videoteleconference lecture, U.S. Consulate, Shanghai, China, May 12, 2003 and "The Department of Homeland Security" videoteleconference lecture, U.S. Consulate, Monterrey, Mexico, July 30, 2003.

[4] See http://www.bundesgrenzschutz.de/Aufgaben/index.php

Bundesgrenzschutz, the combined force would be greater than the CBP and have responsibilities for a border that is much smaller than that of the US.

Moreover, border control policies of EU member states are being integrated into EU institutional structures and the implementation of border controls by member state interior ministries is increasingly coordinated at a European level. The establishment of a single European market in 1986 increased pressure to eliminate internal borders so that trucks and tourists would not be held up by passport inspections. Aspirations for free movement within the EU were paired with the erection of a common external border. So, a subset of EU member states signed the 1990 Schengen Convention that eliminated border checks among its members at the same time that it called for a common visa policy, harmonization of polices to deter illegal migration and an automated Schengen Information System (SIS) to coordinate actions regarding individuals who have been denied entry. Title VI of the 1992 Maastricht Treaty formalized longstanding cooperation among the member states regarding border controls, migration and asylum. Cooperation in the fields of Justice and Home Affairs (JHA) formed one of three "pillars" of the EU along with the First Pillar of the original European Community and the Second Pillar of Common Foreign and Security Policy (CFSP). The pillar structure effectively kept this cooperation on an "intergovernmental basis" outside of the original Treaty on European Community (TEC). The 1997 Amsterdam Treaty set out a plan for the incorporation of the Schengen Convention into the EU treaties and called for common policies and joint actions on visas, asylum, immigration and external border controls to be put under Community procedures and into the Community legal framework. This process is projected to take place over a five-year period beginning when the Amsterdam Treaty entered into force on May 1, 1999. Should the member states eventually approve all of the proposed legislation, the initiation of most

immigration and border control policies will move from member state capitals to the European Commission in Brussels in May 2004.

In the immediate aftermath of the attacks on the World Trade Center and the Pentagon, the extra-ordinary European Council of Sept. 21 invited member states to strengthen controls at external borders and strengthen surveillance measures provided for in the Schengen Convention. The Council advocated vigilance when issuing identity documents and residence permits, recommended more systematic checking of identity papers for document fraud, asked for more input to the Schengen Information System (SIS) from member states and asked for consular cooperation and stepped-up information exchanges between member states regarding visas (European Council 2001).

Shortly thereafter, the Justice and Home Affairs Council began discussions of developing a common border police force, which would involve the development of a harmonized curriculum for training border control officials and the development of a European Border Guard School. Despite the momentum behind the concept, and the support of states such as Germany and Greece, proposals for common border guard were blocked at the 2001 December Laeken European Summit because, as Swedish Prime Minister Goran Persson explained, EU leaders did not want an additional layer of bureaucracy (MNS 2002). Nevertheless, bilateral joint border patrols continue as well as bilateral arrangements for cooperation to deploy assistance to address sudden influxes of illegal migration into fellow member states. Additionally, the integration of border management is going forward with plans for a "European Agency for the Management of Operational Co-Operation at the External Borders of the European Union." This agency would co-ordinate the implementation of common policies by member state border police but not have policymaking or implementing powers of its own. It is expected that the agency will be

established in one of the new member states at the beginning of 2005 with a staff of 30 and initial budget of 6 million Euro (European Commission 2003).

The Schengen Information System (SIS) is a critical component of the Schengen Convention designed to enforce the common external border and build confidence in this common border so as to enable member states to remove all internal border controls among signatory states. Integration into the SIS is necessary before provisions of the Schengen Convention become effective for any signatory state. All EU member states (except the UK) plus Norway and Iceland are connected to the system. The SIS contains data on illegal migrants, lost and false travel documents, wanted or missing persons, stolen goods and counterfeit notes. As of June 2002, approximately 10 million people were listed in the SIS. Most entries were for forged or stolen passports and IDs but 1.3 million were entered into the alert system as convicted and suspected criminals (European Report 2002). The SIS can only electronically transmit text and figures, not photos and fingerprints (European Report 2002a). Since the SIS is only capable of working with no more than 18 members states and cannot handle the increased data processing demands of EU enlargement, the Europeran Commission has proposed the Schengen Information System II (SIS II). SIS II is planned to be deployed by the beginning of 2007 with a 147 million Euro budget for system development and 70 million Euro for management. In addition to increase data capacity, the planned SIS II will be able to store digital images and biometric data and answer police requests within five seconds (European Report 2003). Concerned with SIS II's new capabilities as well as its potential use more often by more law enforcement agencies, the European Parliament issued a recommendation that calls for: EU-wide access rules and an agency with representatives from EU institutions to control SIS; access governed by the principle that data should only be used for the purpose it was originally

requested; better information for citizens about SIS II and a public debate about its development (European report 2003a).

Proposals were also put forward for the development of a European visa identification system as the September 11th attacks raised concerns about the growing illegal migrant population living in Europe and the prospect of terrorists being smuggled into the EU or entering by visa fraud. The European Commission proposed a system featuring a common online database that would complement secure identity documents. A digital photo would be stored in addition to data that is already gathered in visa applications. Travel documents, such as passports, would also be scanned in order to detect any subsequent alterations. Stored images could also be used to get new travel documents should an individual try resist deportation by attempting to hide his or her identity and nationality by destroying travel documents, which were used to enter the country (European Commission 2001b). In June 2002, the Spanish Presidency put forward a proposal to the Council for creating a "Visa Information System" (European Report 2002c). Subsequently, Germany and the Benelux countries proposed a uniform format visa incorporating anti-counterfeit features and biometric data such as fingerprints or iris scans stored on a microchip embedded in the document (European Report 2003b), which would thereby provide more precise data to be shared through the proposed visa information system. In September 2003, the European Commission proposed the incorporation of biometrics into visas and resident permits for third country nationals. Following the ICAO standard for machine-readable travel documents, the Commission chose a digital facial image as the primary biometric. Fingerprints were selected as secondary biometric for superiority in background checks and one-to-many searches (European Commission 2003a)

In response to the Sept. 11th 2001 attacks, the German government passed a first package of anti-terrorism legislation on Sept 19, 2001 which provided 3 billion DM to upgrade national security and included provisions to improve the screening of airport personnel and eased data protection laws, thereby giving relevant authorities access to intelligence and other government databases (details at: *Bundesregierung* 2002). More comprehensive measures were also proposed in a second package, which ultimately contained measures to tighten border controls and identify extremists as well as to improve the security features in personal identification documents and passports (details at: *Bundesregierung* 2002a). As the Cabinet of the German government approved the first package of anti-terrorist measures on Sept 19, 2001 Interior Minister Schily said that the central registry for foreigners and visa data should be made more accessible, while Cem Ozdemir, the Green Party's spokesperson for domestic affairs at the time, argued that the efficacy of any changes in data privacy rules must be first examined (FAZ 2001). Another point of controversy within the SPD/Alliance90/Green coalition government concerned Minister Schily's proposal on biometric data in the second anti-terrorism package of legislation. The Interior Ministry originally demanded inclusion of fingerprint data in identification documents and passports while the Greens proposed using hand and facial geometric data. A compromise emerged to leave open the type of biometric data used while agreeing that the ban on fingerprints in the passport law be lifted (FAZ 2001a). The Greens won further concessions in that biometric data on ID cards and passports would not be recorded in a central data bank, meaning that this data could only be used for verification of identity and not for data-mining in criminal investigations (FAZ 2001b). The second package was passed on Dec. 20, 2001 and went into effect on Jan. 1, 2002. Additional provisions have been made to establish a central database of passport photos to thwart identification substitution, reduce restrictions on

exchanging data, particularly between carriers and authorities on passenger bookings, and selective fingerprinting of visitors upon arrival (IOM 2002).

Border control in the UK is the responsibility of Home Office's Immigration and Nationality Directorate (IND), which has a permanent staff of just over 11, 000 (Home Office 2003). By virtue of the fact that the United Kingdom is an island nation and not a Schengen Convention signatory state, border control primarily involves inspections of some 81,000 ships and aircraft and 90 million passengers per year. (Home Office 2000/2001). In order to detect visa abuse and document fraud at ports of entry as well as to intercept potential terrorists, new immigration and asylum legislation announced in April 2002 includes provisions that enable data sharing between government departments and government and the private sector to facilitate data-mining for profiling and detecting high-risk passengers (IOM 2002). The legislation also set up "right to carry" schemes whereby carriers must confirm that passengers do not present a security risk nor are at risk of breaking immigration law before these passengers are permitted to board UK-bound airplanes. Such carrier sanctions complement efforts to automate immigration controls through a combination of data-sharing and the use of biometric identification systems to speed legitimate passengers through and allow border control officers to concentrate their efforts on more high risk travelers (Home Office 2002). The UK also developed a new "Borderguard" system, which uses electronic recording and facial recognition technology to detect forged documents and uncover abusive asylum claims (Home Office 2002a). The overhaul of British immigration and asylum legislation also includes measures to issue smart cards to asylum applicants for identification and tracking as well as to use biometrics to help identify potential terrorists among asylum seekers (IOM 2002). In November 2003, Home Secretary Blunkett

proposed a national ID card (which for most UK nationals would be a passport) that would include personal data, a digital photo and a biometric such as a fingerprint (Home Office 2003a).

The border control authorities of the EU and its member states collectively have more staff, resources and, in some ways, more "proactive" border control policies than US border control authorities within the Department of Homeland Security. Of course this is partly due to the legacy of controlling borders between EU member states – border controls that have largely been lifted with the implementation of the 1990 Schengen Convention. Should further bilateral and European-wide agreements be reached, tens of thousands of current EU member state border guards (e.g. a large portion of the German *Bundesgrenschutz*) may be redeployed as internal border controls with the EU's new member states are lifted in the coming years and the EU's common external border is moved eastward. Alternatively, these border guards' missions could be shifted toward internal enforcement of immigration policies (i.e. deportation, investigations, workplace enforcement). The EU and EU member states are also supporting border security with information technology deployments similar to that of the US. As in the US, it is unlikely that domestic political changes in government will reverse increased border security measures, given that the German and UK initiatives mentioned above were undertaken by Social Democratic and Labour governments whose Conservative opponents have had even tougher positions on immigration and border controls.

Advanced Passenger Information

In order to pick out potential terrorists from growing flows of travelers, the Aviation and Transportation Security Act passed by the US Congress in the Fall of 2001 requires that airlines with US-bound international flights electronically submit a passenger manifest with data

including full name of each passenger, date of birth, sex, passport number and country of issuance, US visa number or alien card number and "Such other information as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety." The act also mandates that "The carriers shall make passenger name record information available to the Customs Service upon request."[5] The subsequent 2002 US Enhanced Border Security and Visa Entry Reform Act requires commercial airlines and ships to electronically submit passenger and crew manifests before arrival to the US via the Advanced Passenger Information System (APIS), sets out fines for non-compliance and loss of landing rights for those airlines that have not paid their fines.[6]

In order to comply with these regulations, US-based airlines gave access to their Passenger name record (PNR) databases to the US Customs Service. PNR data is created each time a passenger books a flight and it is stored in the airlines reservation systems. The number of data fields and types of data in those fields vary across airlines. Patriotically motivated to help in government counter-terrorism efforts, scrambling to meet a wide variety of aviation security requirements while at the same time dealing with a major downturn in their business, many US-based airlines opted to simply give database passwords to US Customs which allowed Customs to "pull" all PNR data rather than select and "push" a subset of that data which met specific Customs' requests. Although much of the required PNR data is also printed out on passenger tickets and have access to this data when the traveler presents his or her ticket and passport at the port of entry, advanced electronic submission of PNR data allows screening of passengers while US-bound planes are in flight and thereby enables faster processing of passengers through border

[5] Section 115 of the ''Aviation and Transportation Security Act,'' Public Law 107–71, Nov. 19, 2001
[6] Section 402 of the ''Enhanced Border Security and Visa Entry Reform Act of 2002,' Public Law 107–173, May 14, 2002.

controls. Hence, US-based airlines had the added incentive to grant unlimited access in order to expedite passenger arrival processing in their US operation hubs.

The US Customs Service also requested PNR data from European-based airlines. While some have voluntarily provided requested PNR data, several airlines resisted, contending that it would be a violation of EU data protection rules. Essentially, European airlines were presented with choice of either breaking US laws, face fines and potentially loose landing rights or violate EU and EU member state data protection laws and face fines. Discussions between the European Commission and the US Customs Service yielded US compliance extensions for these airlines until March 5, 2003, by which time the EU and the US arrived at an interim "arrangement" stipulating a number of benchmarks that would have to be met before data could be distributed, including: to whom the data was being transmitted; how long the data would be maintained; with whom the data would be shared; etc. If these benchmarks were not met then the data could not be transmitted outside the EU (European Commission-US Customs 2003; CBP 2003). The European Parliament promptly voted overwhelming in favor of a resolution criticizing the European Commission for putting aside EU data protection rules and doing so in an arrangement that lacked a legal basis. Parliament expressed its intent to pressure the Commission in order to obtain a legal agreement, such as treaty, to accommodate US requests for PNR data.

The European Commission and the DHS engaged in months of negations to secure legally sound agreement in the form of a Commission "adequacy decision" that data were adequately protected and corresponding "Undertakings" issued by the DHS, which promise that data would receive agreed-to treatment. At the outset, the DHS wanted data transferred from 60 fields, the Commission wanted to limit this number to 25. The DHS wanted to use data to investigate and prevent not only terrorism but all serious crime, the Commission wanted to limit

data use to prevent terrorism only. Initially the DHS wanted to maintain data for seven years, the Commission wanted data to be erased after flights were completed (Bolkestein 2003; Waterman 2003; 2003a). After months of negotiations, on Dec. 16, 2003, the DHS Border and Transportation Directorate initialed an agreement with the European Commission on legal transfer of PNR data. Key features of the agreement include: transfer of 34 elements of PNR data; use restricted to preventing and combating terrorism and serious crimes that are transnational (i.e. not domestic crime); retention of data for up to 3.5 years; a 3.5 year sunset provision for the agreement itself; redress to passengers through the newly established DHS Privacy Office with the possibility of EU data protection authorities representing EU citizens (Bolkestein 2003; DHS 2003).

The DHS had also wanted PNR data to be submitted before US-bound flights departed for input into the Transportation Security Administration's Computer-Assisted Passenger Pre-Screening System (CAPPS II), which conducts automated risk assessments of all airline passengers using PNR data together with commercially available databases and intelligence. The Commission insisted that the agreement only covered data submission to CBP and resisted wholesale data transfers from CBP to TSA. Commissioner Bolkestein reported to the Parliament that "the arrangement will not cover Computer-Assisted Passenger Pre-Screening System (Bolkestein 2004)." However, when the Commission decision (European Commission 2004) and US "Undertakings" (CBP 2004) were issued, it became clear the Commission accepted the Undertakings' provision that CBP may transfer PNR data on a bulk basis to TSA for the purposes of testing CAPPS II. It has been difficult for TSA to get PNR data from airlines to test CAPPS II, especially after Jet Blue Airlines was sued by passengers because the airline violated its own privacy policy by providing PNR data to a Defense Dept contractor (apparently with

some help from the TSA) in order that the firm could test a data-mining system (Adcock 2003). According to a February 2004 report issued by the US Government Accounting Organization, "TSA is currently behind schedule in testing and developing initial increments of CAPPS II, due in large part to delays in obtaining passenger data needed for testing from carriers because of privacy concerns (GAO 2004)." In response to the GAO report, Homeland Security Undersecretary Asa Hutchinson argued, "I do think the GAO Report, also, failed to recognize international progress that has been made in the area of receiving data for testing purposes. We have been very successful and worked very hard in working with European Commission on receiving a preliminary agreement that we would have the transfer of PNR Data that would include an ability to test for the CAPPS II system and that has not been finalized yet and still has to be approved but we've made enormous strides in being able to utilize the European data for that purpose (Hutchinson 2004).

Soon thereafter, the European Parliament called upon the Commission to withdraw the draft decision, criticizing the draft decision for, among other things, enabling transfer of PNR data to TSA for test purposes (European Parliament 2004). Concerns were expressed that TSA is trying to get data from European Airlines that it cannot get domestically. Noting that the protection of privacy is not a fundamental right under the US Constitution and "no legal protection is currently granted in the case of data relating to non-US (and in particular European) passengers, nor is there any right of legal redress should the measures restricting the freedom to travel be abused" the Parliament argues, that the Commission's decision, "Presents the risk that millions of European passengers will be subject to comprehensive surveillance and monitoring by a third country. (European Parliament 2004: 4-5)." As long as the European Council continues to support the Commission on this issue, the Parliament cannot stop the transfer of

PNR data on its own authority, however, persistent Parliamentary objections, hearings and engagement of advocacy groups may undermine support in individual EU member states and set the stage for a legal challenge in the European Court of Justice.

Interestingly, if EU member states were to demanded PNR data from US-based airlines, there is no legal framework for permitting this and the airlines could easily refuse. The CBP "Undertakings" state that, "In the event that the European Union decides to adopt an airline identification system similar to that of the US Government, which requires all carriers to provide European Authorities with access to PNR data for persons whose current travel itinerary includes a flight to, from or through the European Union, CBP would encourage US-based airlines to cooperate" (CBP 2004: 16, para. 45). It stands to reason that US-based airlines that have already given access to US Customs and Border Protection would not resist giving access to European authorities, however, the lawsuits against Jet Blue may prejudice other airlines against voluntarily giving access to PNR data to European border control authorities unless specifically required by new US legislation.

Although the Commission did not satisfy the European Parliament on many points of the PNR transfer agreement, it did follow through with Parliament's recommendation to move the issue to a multilateral forum. Partly motivated by the fact that Canada and Australia have also passed legislation requiring advanced submission of PNR data, Ireland, on behalf of the EU, will put forward a proposal for an international framework for the transfer of PNR data at an upcoming meeting of the International Civil Aviation Organization (Ireland 2004). Given the increasing concern over the privacy of PNR data raised in the US Congress (e.g. Collins, 2003) and by the European Parliament, there may be major limitations to further international PNR

data transfer without global multilateral agreements and implementing legislation on the national level.

Document security, biometrics and the future of visa-free travel between the US and EU.

In response to the attacks of September 11, 2001 and the subsequent attempt by a UK national, Richard Reid, to detonate a bomb hidden in his shoes while on a transatlantic flight, some US legislators raised the possibility of eliminating the program that allows nationals of 27 states (including all EU member states except Greece) to enter the United States without a visa for a stay of up to 90 days (Carr 2002). Instead of abolishing the Visa Waiver Program, Congress passed provisions designed to increase its security. The USA Patriot Act required that Visa Waiver Program countries have machine-readable passports by October 1, 2003[7] and the Enhanced Border Security and Visa Entry Reform Act goes a step further by conditioning countries' participation in the Visa Waiver Program on the issuance of machine-readable, tamper-resistant passports containing biometric data and sets a deadline of Oct 26, 2004. Since many European states could not make the Patriot Act deadline for machine-readable passports, the State Department gave them a one-time waiver until Oct. 26, 2004.

The Enhanced Border Security and Visa Entry Reform Act in essence sets out a two-part requirement for the Visa Waiver Program countries and their nationals:

> (c) TECHNOLOGY STANDARD FOR VISA WAIVER PARTICIPANTS.—CERTIFICATION REQUIREMENT.—Not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program established under section 217 of the Immigration and Nationality Act shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and

[7] Section 417 of the" Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001," Public Law 107-56, Oct. 26, 2001.

> document identifying standards established by the International Civil Aviation Organization. ….
> USE OF TECHNOLOGY STANDARD.—On and after October 26, 2004, any alien applying for admission under the visa waiver program under section 217 of the Immigration and Nationality Act shall present a passport that meets the requirements of paragraph (1) unless the alien's passport was issued prior to that date.[8]

The US Congress deferred to the International Civil Aviation Organization (ICAO) on stetting the biometric standard and it was not until May 28, 2003 that the ICAO announced an agreement - facial recognition plus optional fingerprints and/or retina scans. The ICAO biometric standard "blueprint" has four parts: the primary facial recognition biometric; contactless integrated circuit (IC) chips (at least 32K bytes) for the electronic storage of biometric data on the travel document; a logical data structure that specifies instructions for programming the contactless IC chip and a public key infrastructure to secure the electronic data on the chips (ICAO 2003).

The contectless IC chip and other Radio Frequency Identification (RFID) technologies are central to the vision of the "revolution in border security." The contactless IC chip is part of an RFID system in which data on the IC chip is transmitted via radio waves to a reader. The reader provides the power; the contactless IC chips are passive and do not require batteries. As opposed to machine-readable travel documents that contain data on magnetic strips, a passport with a contactless chip can be read by the reader at a distance, therefore allowing faster transfer of data from the passport. Similar applications include Washington, DC Metro Smartrip cards, which are read by touching a pad on turnstiles triggering deduction of the fare from the digital account on the embedded chip[9] and the New Jersey EZ-pass highway and bridge toll system, toll gates that read the radio waves that bounce back from passive transponders in automobiles and

[8] Section 303 of the ''Enhanced Border Security and Visa Entry Reform Act of 2002,' Public Law 107–173, May 14, 2002.
[9] See http://www.wmata.com/riding/smartrip.cfm

record the passage of enrolled automobiles.[10] As envisioned, holders of new biometric passports issued by Visa Waiver countries will give their passports to CBP inspectors who will simply bring the passport close to the reader. The reader will capture the personal data and the digitized biometric. This information can then be checked against terrorist and law enforcement watch lists. If there are no hits, the inspector can then allow the traveler to continue on through passport control and enter into the US. Similarly, upon exiting within the 90-day limit of the Visa Waiver Program, the traveler will "check out" of the country with a wave of the passport over a reader, possibly even using a self-service kiosk. There are major obstacles to realizing this vision, especially by October 26, 2004, as mandated by Congress.

Even if a Visa Waiver Program country incorporated biometrics on contactless IC chips into its passports in time to comply with the Oct. 26, 2004 deadline, DHS officers at US ports of entry might not have the right equipment to read the data from those passports because there is no agreed-to international standard for guaranteeing interoperability contactless IC chips and RFID readers. Different radio frequencies are used by different companies that make RFID systems and if countries in the Visa Waiver Program begin purchasing these systems before a single RF standard is agreed to, the IC chips in some passports might not be readable by the machinery at the US port of entry or the US might have to invest in as many as 27 different readers for all of the different passports (Williams 2004). The ICAO New Technologies Working Group has produced a technical report that recommends IC chips that conform to ISO standards ISO/IEC 14443 for "proximity" applications and ISO/IEC 15693 for "vicinity" applications. Proximity applications refer to staffed border controls in which the passport holder gives the passport to an inspector for machine reading. Vicinity applications refer to "self-service" inspection in which the passport holder would simply walk past an RFID reader that

[10] http://www.ezpass.com/

would receive the passport data and digitized biometric at a distance and then permit or deny entry or exist automatically (ICAO 2003a). The ICAO Facilitation Division will have an opportunity to decide on a standard at its Mar. 22 –Apr. 2, 2004 meeting in Cairo. If it does so, that will leave six months for Visa Waiver countries to deploy new passports with RFID chips and six months for the US to install the RFID readers that are compatible with those passports at all US air and sea ports of entry.

As of this writing, no Visa Waiver countries currently issue biometric passports meeting the ICAO standard. Since the first part of the requirement in the Enhanced Border Security and Visa Entry Reform Act refers to having a "program" to issue biometric passports, most, if not all, Visa Waiver countries should be able to have programs in place that meet this requirement by Oct. 26, 2004, depending of course on how an acceptable "program" is defined by the US Administration and Congress. One possible solution for EU member states to meet this requirement is the European Commission's Proposal for a Council Regulation on Standards for Security Features and Biometrics in EU Citizens' Passports (European Commission 2004). This proposal for what is commonly referred to a "European Passport" grows out of a long line of initiatives associated with the development of EU citizenship in the 1980s and 1990s, the post-Sept 11, 2001 security initiatives of the European Council (referred to above) and the US requirements for continued participation in the Visa Waiver Program (European Commission 2004: 2-3). From the standpoint of Jonathan Faull, Director General for Justice and Home Affairs at the European Commission, the 25 current and new member states of the European Union will have a biometric passport program in place once the European Council approves the

proposed regulation[11] and all the US needs to do is recognize it as meeting legislative requirements.

While programs may be in place, few Visa Waiver Program countries will be able to meet the second part of the requirement of including biometrics in all new passports issued to their nationals from Oct. 26, 2004 onward. According to Assistant Secretary of State for Consular Affairs Maura Harty, the U.K., France, Germany, Ireland, Italy and Spain will not begin issuing passports with the ICAO standard facial recognition biometric by October 26, 2004. The UK has indicated that it will do so late 2005 while others may not do so until a year after that (Hartly 2004).

If the US were to drop a current EU member state from the Visa Waiver program, that could trigger a chain of events that would end visa-free travel between the US and the EU. Currently all EU member states except Greece are in the US Visas Waiver Program. If, for example, the US would begin to require visas of Spanish nationals, Spain could follow the traditional approach to visa policy, which is to reciprocate and require visas from US nationals. As the EU has a common visa policy, Spain could invoke the solidarity clause of this common policy, which would require visas of all US nationals traveling to the EU. Moreover, since Iceland and Norway are parties to the Schengen Convention and Switzerland has a special arrangement with the Schengen countries, these states would also have to impose a visa requirement on US nationals if they wish to maintain free movement with the other Schengen countries of the EU.

Nine of the ten states entering the EU on May 1, 2004 are not members of the Visa Waiver Program (all except Slovenia). There is a good possibility that the issue of US-EU visa

[11] Response to a question posed after Mr. Faull's presentation at "Fortress America? The Implications of Homeland Security on Transatlantic Relations," American Enterprise Institute, March 4, 2004. http://www.aei.org/events/eventID.758,filter.all/event_detail.asp

reciprocity will come to a head as these states join the EU because once in the EU, any one of them could also invoke the solidarity clause of the common visa policy, should the US persist in not granting their nationals visa-free travel. During his January 2004 visit to the US, Polish President Aleksander Kwasniewski asked President Bush to drop the US visa requirement, which Kwasniewski asserted was too stringent especially for a staunch US ally in the war in Iraq. When the issue came up publicly at a photo opportunity, President Bush referred to "visa rules set by the Congress that are on the books" and suggested the formation of "U.S.-Polish study group" to examine the issue (Loven 2004). Radek Sikorski, a fellow of the American Enterprise Institute who had previously served as Poland's Deputy Minister of Foreign Affairs and Deputy Minister of Defense, put the issue in sharp relief at a March 2004 panel discussion he organized, which included Stuart Verdery, Assistant Secretary for Policy and Planning at the Border and Transportation Security Directorate of the DHS, and Jonathan Faull of the European Commission. From the description of the event: "Citizens of countries that have supported America in Iraq are fingerprinted and photographed on arrival in the United States while visitors from countries where many radical Islamists reside--such as France and Germany--can enter without visas and without being fingerprinted. Should Americans apply the same standards to everyone?"[12]

Politically, it will be increasingly difficult for the DHS to continue ask for fingerprints from Poles and not from the French and Germans. Polish-American lobbying[13] has already prompted Republican Congresswoman Nancy Johnson to introduce a resolution in Congress to include Poland into the Visa Waiver Program and her press release pointed notes that

[12] The description and a video of the event are at: http://www.aei.org/events/eventID.758,filter.all/event_detail.asp.
[13] See for example, the Polish-American Congress agenda at: http://www.polamcon.org/legislative-agenda0104.htm

"Approximately nine million Americans of Polish ancestry live in the United States."[14] Moreover, every ethnic group in the US whose co-ethnics need visas to enter will make the same kinds of arguments to their representatives. The perceived double standard could also be addressed if the US would require Visa Waiver Program countries to include fingerprint biometrics in addition to digital photographs in their passports. Stuart Verdery noted the security benefits of adding fingerprint biometrics because it would permit checks against existing law enforcement fingerprint databases whereas there is as yet little in the way of equivalent facial recognition biometric databases.[15] If the US were to require additional fingerprint biometrics in Visa Waiver country passports, Jonathan Faull warned that EU member states would reciprocate and require fingerprints of US nationals.[16]

Another possible scenario is that a Visa Waiver country that does meet the requirement to issue biometric passports by Oct. 26, 2004 could follow the principle of reciprocity and require the same of US nationals – a requirement that the US State Department is not prepared to meet. While all new US passports include digital photographs that are much more difficult to physically alter, the US is not required by legislation to include ICAO standard biometrics in US passports. When in November 2003 DHS Undersecretary Asa Hutchinson was asked if US could meet the requirement for our own Visa Waiver Program on October 26, 2004, he referred to having a passport "program in place" by then.[17] According to subsequent testimony by

[14] See "Johnson: Polish Visitors Need No Visa, Introduces Resolution Urging Poland Be Added to Visa Waiver List," Press release, February 13, 2004 at: http://www.house.gov/nancyjohnson/pr_polishvisitors.htm.
[15] Response to author's question posed after Mr. Verdery's presentation at Fortress America? The Implications of Homeland Security on Transatlantic Relations," American Enterprise Institute, March 4, 2004. http://www.aei.org/events/eventID.758,filter.all/event_detail.asp
[16] Response to author's question posed after Mr. Faull's presentation at "Fortress America? The Implications of Homeland Security on Transatlantic Relations," American Enterprise Institute, March 4, 2004. http://www.aei.org/events/eventID.758,filter.all/event_detail.asp
[17] In response to author's question at the panel discussion, "New transatlantic challenges in the changed international security environment: American and European views on cooperation on migration," The German Marshall Fund of the United States, October 27, 2003.

Assistant Secretary Hartly, the State Department has a pilot program to produce its first passports that use the ICAO facial recognition standard in October 2004 and plans to have all new passports issued meet this standard by the end of 2005 (Hartly 2004). Therefore, the US could not meet the requirements of its own Visa Waiver program because it will still be issuing passports without biometrics after the Oct. 26, 2004 deadline.

If the US holds fast to the Oct. 26, 2004 deadline for both parts of the biometric passport requirement, most EU states will be dropped from the Visa Waiver Program. Nationals of these states will then have to apply in person at US embassies and consulates for visas and as Deputy Assistant Secretary of State for Consular Affairs, Janice L. Jacobs has stated, "By October 26, 2004, all US visas must incorporate a biometric identifier. In accordance with international standards established by the International Civil Aviation Organization, we have selected facial recognition and electronic fingerprint scanning as the most effective and least intrusive (Jacobs 2003)." A digital photograph and fingerprints will be taken of all visa applicants at US embassies and consulates then they are compared with biometrics collected upon arrival at the port of entry through the US-VISIT program.

While it is a distinct possibility that the US may drop EU member states from the visa waiver program, the prospects for this happening are unlikely because this course of action is very rather costly and problematic for both the US and the EU. According to the US General Accounting Office, "Should the Congress decide to require visas from current visa waiver travelers, State would require more resources, such as personnel and facilities overseas, to handle the resulting increased visa processing and biometric collection workload. State estimates that if the individuals now traveling under the Visa Waiver Program were required to obtain visas, the number of applications would rise by 14 million. We estimated that State's initial costs to process

the additional workload would likely range between $739 million and $1.28 billion, and annual recurring costs would likely range between $522 million and $810 million (GAO 2002)

In her response to questions posed at a January 2004 hearing of the National Commission on Terrorist Attacks Upon the United States, Assistant Secretary Hartly replied that the State Department has enough resources to put in place the infrastructure necessary to collect biometrics from those people currently required to travel with visas to the US. If the Visa Waiver Program were to be eliminated or if the US dropped several EU member states that send large numbers of travelers to the US, she acknowledged that the State Department could not process these additional visa applications. Not only would the State Department have to hire and train a large contingent of new consular officers, in many European countries acquiring the necessary space and physical infrastructure to interview and process visa applicants would take over a year – just about the time when these countries will have their new passports enabling them to once again meet the Visa Waiver Program requirements. In light of these realities, Ms. Hartly suggested that pushing the Oct. 26, 2004 deadline back would be the most financially and logistically realistic option (see Hartly 2004a). Indeed, Bush administration officials and Congressional staffers have formed a group to negotiate the terms of a deadline modification (Williams 2004).

Staring at the prospect of the end of visa free travel between the US and E.U., it is likely that US policymakers will accept the recent EU biometric passport proposal as evidence for a "program" meeting the requirements of the Enhanced Border Security and Visa Entry Reform Act. It is also likely that the Bush Administration and Congress will come to an agreement to push back the October 26, 2004 deadline for the requirement that all new passports issued contain biometrics. To begin with, it is difficult for US to ask EU member states to meet a

deadline that US officials have already admitted the US could not meet itself. Also, the threat of requiring biometric visas of EU nationals "or else" rings somewhat hollow since the US State Department does not have the staffing and resources in place to process the applications, conduct interviews and collect biometrics from the millions of additional visa applicants. In the meantime, international negotiations within ICAO may yield a consensus on one global standard for both passport and visa biometrics, thereby overcoming the double standard for those who need a visa to travel and those who do not.

Conclusion

When EU member states and the U.S. came to loggerheads in the Security Council over military intervention in Iraq, commentators declared that US-EU relations had hit a new low and the prospects for future international cooperation were very bleak. While the US-European diplomatic impasse may have rendered multilateralism moribund in the halls of the United Nations, intensified contacts between US and EU border security officials led to mutual understandings, cooperative informal arrangements and more formal agreements. Transatlantic cooperation on PNR data collection and exchange as well as the setting of biometric standards requires acceptance of mutual constraints on the range of state action in the area of border control – one of the defining aspects of territorial sovereignty.

Further cooperation, however, may be interrupted by differing legal regimes governing privacy and personal data protection. From the standpoint of the European Parliament, the European Commission appears to be willing to compromise to an unacceptable degree on data protection standards for the sake of security and increasing transatlantic cooperation. Interestingly, the imperatives of cooperating with the EU have furthered the development of the

US Department of Homeland Security's privacy protection infrastructure. Similarly, publicity triggered by negotiations with the EU over data protection and contrasts between EU and US policies has helped set the stage for Congress to reconsider some of its mandates to collect and mine passenger data (Young 2004).

In addition to the barriers posed by European data protection laws, increasing cooperation on travel document security and entry-exit tracking systems is also inhibited by strong social norms against fingerprinting citizens who have not committed crimes. The above discussion of German politics regarding biometric data collection provide an example of the barriers that European interior ministers may face should fingerprint biometrics be required on passports for maintaining US Visa Waiver status. But at least the German government has raised the issue of fingerprinting its citizens for the sake of increased security. So far, the US Congress, the State Department and the DHS have largely avoided the issue of collecting fingerprint biometrics from US citizens who wish to travel abroad and have only imposed the requirement on nationals of other states. Requiring a digital photo which is mostly useful for one-to-one identity verification checks is much less politically charged than requiring collection of fingerprint biometrics which are much more useful for one-to-many checks against existing law enforcement databases. Given the longstanding diplomatic practices of visa reciprocity as well as the political dynamics of EU enlargement and American ethnic politics discussed above, US policymakers may soon be presented with the choice of either dropping the fingerprint biometric requirement of foreigners traveling to the US or convincing US citizens who wish to travel abroad to accept fingerprinting. While US (and to a lesser degree EU) policymakers are avoiding the issue of requiring fingerprints from their own citizens, this may be a rather naïve position to maintain.

The technical capabilities for the US and EU member states to gather and exchange tremendous volumes of data regarding travelers and migrants is rapidly becoming available. It is clear that in the post-September 11th environment, legislators, their constituents and administrators are willing to train those technologies on the foreigners entering their countries. It is not so clear that there is equivalent political will for accepting other states' use of the same technologies when they themselves are the "foreigners" subject to data submission requirements. Given that transatlantic deals between the EU and the US on PNR data transmission and biometric standards may be politically unsustainable in the long term, international agreements on a global basis may be the only long-term option for border control authorities to get the data their information systems need to make the envisioned "revolution in border security" into a practical reality that may better secure their national borders in an era or increasing globalization.

References:

Adcock, Sylvia 2003. "JetBlue: Government Asked for Data; Release Prompts 2 Lawsuits," *Newsday*, September 24, 2003.

Bolkestein 2003. "Frits Bolkestein Member of the European Commission in charge of the Internal Market, Taxation and Customs EU/US talks on transfers of airline passengers' personal data Address to European Parliament Committees on Citizens' Freedoms and Rights, Justice and Home Affairs and Legal Affairs and the Internal Market Strasbourg, 16th December 2003," Commission of the European Communities, *RAPID*, SPEECH: 03/613, 16th December 2003

Bundesregierung 2002. "Erstes Anti-Terror-Paket," Innenpolitik, Presse- und Informationsamt der Bundesregierung, Sept. 1, 2002, downloaded Feb. 1, 2003 at: http://www.bundesregierung.de/Themen-A-Z/Innenpolitik-,7418/Erstes-Anti-Terrorpaket.htm

Bundesregierung 2002a. "Zweiten Anti-Terror-Paket in Kraft getreten" Innenpolitik, Presse- und Informationsamt der Bundesregierung, Jan. 1, 2002, downloaded Feb. 1, 2003 at: http://www.bundesregierung.de/Themen-A-Z/Innenpolitik-,7419/6

Carr, Rebecca 2002. "Concern Grows over INS Visa Waiver Program," Cox News Service February 28, 2002.

CBP 2003. "Results of talks on 4 March 2003 between the European Commission and US Customs and Border Protection (CBP) with regard to Passenger Name Record (PNR) sensitive data," Department of Homeland Security: Customs and Border Protection, Mar. 4, 2003.

CBP 2004. "Undertaking of the Department of Homeland Security Bureau of Customs and Border Protection (CBP)," annex I to European Commission 2004.

Collins, Susan 2003. "Senators Call on TSA to Explain its Role in Obtaining Sensitive Airline Passenger Information: Did TSA Ask JetBlue to Provide Data for Screening Program?" Press Release from the Office of Sen. Susan Collins, Chair of Senate Committee on Government Affairs, February 13, 2004.

DHS 2003. "Fact Sheet: Homeland Security and European Commission Reach PNR Agreement" Department of Homeland Security, Office of the Press Secretary, December 16, 2003. Downloaded Jan. 20, 2004 at: http://www.dhs.gov/dhspublic/display?content=3036

DHS 2004. Homeland Security Budget in Brief: Fiscal Year 2005. Downloaded on Mar. 7. 2004 at: http://www.dhs.gov/dhspublic/display?content=3131

European Commission 2001b. "Communication From the Commission to the Council and the European Parliament on A Common Policy on Illegal Immigration," Commission of the European Communities, Brussels, 15.11.2001, COM(2001) 672 final.

European Commission 2003. "Establishing a European Agency for the Management of the Operational Co-Operation at External Borders," RAPID Press Release IP: 03/1519, Nov. 11, 2003.

European Commission 2003a. "Commission's proposal on biometric identifiers for visa and residence permit for third country nationals," RAPID Press Release, IP/03/1289, Sept. 24, 2003.

European Commission 2004. "Proposal for a Council Regulation on Standards for Security Features and Biometrics in EU Citizens Passports" COM (2004) 116 Final, 2004/0039 (CNS), European Commission, Brussels, February 18, 2004.

European Commission 2004. Draft Decision on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection. European Commission (C5-0000/2004)

European Commission-US Customs 2003. Joint Statement of the European Commission and U.S. Customs Service, Brussels, February 17/18, 2003. Downloaded Mar. 20, 2003 at: http://www.europa.eu.int/comm/external_relations/us/intro/pnr-joint03_1702.htm

European Council 2001. "Conclusions and Plan of Action of the Extraordinary European Council Meeting on 21 September, 2001."

European Parliament 2004. "Motion for a Resolution on the Draft Commission Decision noting the Adequate Protection of Personal Data Contained in the PNR of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection (C5-0000/2004)" Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Feb. 17, 2004.

European Report 2002. "Justice and Home Affairs: Council Moves to Add Al-Qaeda Members to Schengen Information System," *European Report* (June 26, 2002).

European Report 2002a. "Danish Presidency Proposes Intra-Police E-mail System," *European Report*, July 24, 2002.

European Report 2002c. "EU Visa Database Takes Shape," *European Report*, June 5, 2002

European Report 2003. "Commission wants New Schengen Data base to Store Biometrics, *European Report*, No. 2828, Dec. 13, 2003.

European Report, 2003a. "Parliament Says Schengen Data Needs to Be Controlled Better," *European Report*, 2822, Nov. 22, 2003

European Report, 2003b "Council Moves to Make Visas More Forgery Proof," *European Report*, Jan. 18, 2003.

Faull, Jonathan 2004. Jonathan Faull's response to author's question posed after Mr. Faull's presentation at "Fortress America? The Implications of Homeland Security on Transatlantic

Relations," American Enterprise Institute, March 4, 2004.
http://www.aei.org/events/eventID.758,filter.all/event_detail.asp

FAZ 2001. "Cabinet Approves Emergency Laws" *Frankfurter Allgemeine Zeitung* Sep. 19, 2001. Downloaded on Feb 1, 2003 at:
http://www.faz.com/IN/INtemplates/eFAZ/default.asp

FAZ 2001a. "Coalition Experts Approve Schily's Anti-Terror Package" *Frankfurter Allgemeine Zeitung*, Oct. 26, 2001. Downloaded on Feb. 1, 2003 at:
http://www.faz.com/IN/INtemplates/eFAZ/default.asp

FAZ 2001b. "Coalition Partners Reach Consensus on Anti-Terror Package" *Frankfurter Allgemeine Zeitung*, Oct. 26, 2001. Downloaded on Feb. 1, 2003 at:
http://www.faz.com/IN/INtemplates/eFAZ/default.asp

Flynn, Steven E. 2000. "Beyond Border Control," *Foreign Affairs*, Vol. 79 no. 6 (Nov./Dec.), pp. 57-68.

GAO 2002, "Implications of Eliminating the Visa Waiver Program," General Accounting Office, GAO-03-38, Nov. 2002.

GAO 2004. "Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges," General Accounting Office GAO-04-385 February 13, 2004.

Hartly 2004. Statement by Assistant Secretary of State for Consular Affairs Maura Harty Before the House Select Committee on Homeland Security, Subcommittee on Infrastructure and Border Security, January 28, 2004.

Hartly, Maura 2004a. Answer to question during testimony of Maura Hartly, Assistant Secretary for Consular Affairs, Department of State at the Seventh public hearing of the National Commission on Terrorist Attacks Upon the United States, January 26, 2004.

Hart-Rudman Commission 2001. U.S. Commission on National Security/21st Century co-chaired by Gary Hart and Warren Rudman, *Road Map for National Security: Imperative for Change: The Phase III Report of the U.S. Commission on National Security/21 st Century*, February 15, 2001.

Hillman, G. Robert, 2002. "Ridge: Support Broad for Agency Merger; Security Chief Expects Bush to Move Forward with INS-Customs Plan," *The Dallas Morning News*, April 23, 2002.

Home Office 2000/2001. "Controlling Admissions" Chapter 3, *Immigration and National Directorate Annual Report 2000/2001*, Downloaded Feb. 17, 2003
http://194.203.40.90/default.asp?pageID=1205

Home Office 2002. "Trust and Confidence in our Nationality, Immigration and Asylum system - Bill published," April, 12, 2002. Downloaded Feb 3, 2003 at: http://194.203.40.90/news.asp?NewsId=132&SectionId=1

Home Office 2002a. "Home Secretary sees operation of new high-tech border controls at Dover," and Nationality Directorate of the Home Office (June 17, 2002). Downloaded Feb. 20, 2003 at: http://194.203.40.90/news.asp?NewsId=159&SectionId=1

Home Office 2003. *Home Office Departmental Report 2003*. Downloaded Mar. 10, 2004 at: http://www.homeoffice.gov.uk/docs2/annrep2003.html

Home Office 2003a. "David Blunkett: National ID Card Scheme to be Introduced," Home Office Press Release, ref #307/2003, Nov. 11, 2003. Downloaded Feb 3, 2004 at: http://www.homeoffice.gov.uk/n_story.asp?item_id=675

Hutchinson, Asa 2004. "Undersecretary Hutchinson's Remarks at a CAPPS II Media Roundtable, Feb. 13, 2004" Downloaded Mar. 7, 2004 at: http://www.dhs.gov/dhspublic/display?content=3166

ICAO 2003. "Biometric Identification to Provide Enhanced Security and Speedier Border Clearance for the Travelling Public," International Civil Aviation Organization, PIO/2003 (28 May 2003). Downloaded Nov. 20, 2003 at http://www.icao.int/icao/en/nr/2003/pio200309.htm

ICAO 2003. "Use of Contactless Integrated Circuits in Machine Readable Travel Documents," International Civil Aviation Organization Technical Report, Version 3.1, April 16, 2003.

INS 2002. "INS Restructuring Plan – Next Steps," INS Fact Sheet, April 17, 2002. Downloaded on April 20, 2002 at: http://www.ins.usdoj.gov/graphics/publicaffairs/factsheets/restruct_FS.htm

IOM 2002. International Organization for Migration, "International Comparative Study of Migration Legislation and Practice" (April 2002).

Ireland 2004. "An International Framework for the Transfer of Passenger Name Record (PNR) data," Working Paper, Presented by Ireland on Behalf of the European Community and its Member States, Facilitation Division, ICAO Cairo, Egypt, 22 March to 2 April 2004.

Kerry, John 2004. "Fighting a Comprehensive War on Terrorism," Remarks by Senator John Kerry at the Ronald W. Burkle Center for International Relations, University of California at Los Angeles, February 27, 2004. http://www.johnkerry.com/pressroom/speeches/spc_2004_0227.html

Lieberman, Joseph 2002. "Statement by Chairman Lieberman on Establishing A National Department of Homeland Security," April 11, 2002 downloaded April 20, 2002 at: http://www.senate.gov/~lieberman/press/02/04/2002411658.html

Loven, Jennifer 2004. Polish leader appeals to Bush over visas, *Boston Globe* Jan. 27, 2004.

MNS 2002. "No Significant Progress on the Dossiers Concerning Immigration and Asylum - Proposal to Create Border Guard Blocked," *Migration News Sheet*, No. 226/2002-01 (January 2002), pp. 1-2.

Waterman, Sean 2003. "Europeans meet on Passenger Data Row," *United Press International*, Nov. 23, 2003.

Waterman, Sean 2003. "U.S., EU Reach Passenger Data Deal," *United Press International,* Dec. 16, 2003.

Williams, James 2004. Response to author's question at presentation at the event "Entering America: Challenges Facing the US-VISIT Program," Heritage Foundation, March 1, 2004 http://www.heritage.org/Press/Events/ev030104a.cfm

White House 2002. "The Department of Homeland Security," Office of Homeland Security, White House, issued June 6, 2002. Downloaded Jan. 25, 2004 at: http://www.dhs.gov/dhspublic/display?theme=59

White House 2002a. "National Strategy for Homeland Security" Office of Homeland Security White House, issued July 16, 2002. Downloaded on Jan. 25, 2002 at: http://www.whitehouse.gov/homeland/book/index.html

White House 2002b. "Fact Sheet: Border Security," The White House, Jan. 25, 2002. Downloaded on Jan 27, 2002 at: http://www.whitehouse.gov/news/releases/2002/01/20020125.html

Young, Don 2004. "Status Of Airline Passenger Screening System CAPPS II To Be Focus Of Congressional Hearing" Press release, U.S. Rep. Don Young, Chairman, U.S. House Committee on Transportation and Infrastructure, March 4, 2004. Downloaded Mar. 10, 2004 at: http://www.house.gov/transportation/press/press2004/release14.html