TransAtlantic Council on Migration

A Project of the ***Migration Policy Institute***

A New Architecture for Border Management

By Demetrios G. Papademetriou and Elizabeth Collett

mpi
MIGRATION POLICY INSTITUTE

TRANSATLANTIC COUNCIL ON MIGRATION

A New Architecture for Border Management

Demetrios G. Papademetriou

Elizabeth Collett

March 2011

mpi
MIGRATION POLICY INSTITUTE

Acknowledgments

The authors would like to thank the following Migration Policy Institute (MPI) staffers: Ashley Challinor for her help compiling the appendix, Natalia Banulescu-Bogdan and Madeleine Sumption for their extremely useful comments, and Michelle Mittelstadt and Burke Speaker for their edits. The authors also thank the numerous experts and practitioners who gave up their time to discuss these issues.

This report was commissioned by the Transatlantic Council on Migration for its meeting held in November 2010 in Washington, DC. The meeting's theme was "Restoring Trust in the Management of Migration and Borders" and this paper was one of the key reports that informed the Council's discussions.

The Council is an initiative of the Migration Policy Institute undertaken in cooperation with its policy partner, the Bertelsmann Stiftung. The Council is a unique deliberative body that examines vital policy issues and informs migration policymaking processes in North America and Europe. The Council's work is generously supported by the following foundations and governments: Carnegie Corporation of New York, Open Society Foundations, Bertelsmann Stiftung (Policy Partner), the Rockefeller Foundation, the Barrow Cadbury Trust (UK Policy Partner), the Luso-American Development Foundation, the Calouste Gulbenkian Foundation, and the governments of Germany, Greece (through 2010), the Netherlands, and Norway.

For more on the Transatlantic Council on Migration, please visit: www.migrationpolicy.org/transatlantic.

Cover Photo: US surveillance tower in Nogales, AZ by Jonathan McIntosh
Cover Design: Danielle Tinker, MPI
Typesetting: April Siruno, MPI

Suggested citation: Papademetriou, Demetrios G. and Elizabeth Collett. 2011. *A New Architecture for Border Management.* Washington, DC: Migration Policy Institute.

Table of Contents

Executive Summary

The explosion in global travel and the dawning of the age of risk have exposed substantial weaknesses in border management systems. This has led to the emergence of a new border architecture that seeks to respond effectively to the seemingly competing demands of facilitating mobility while better managing the risks associated with cross-border travel (e.g., terrorism, organized crime, and the entry of unwanted migrants). Information and technology are the centerpieces of this new architecture. Their fundamental aim is to effectively identify and "clear" legitimate travelers quickly so as to free up and focus the bulk of resources on travelers about whom there is not enough information and those who are thought to be posing a threat. And, of course, these objectives must be achieved as far away from the physical border as possible — in a manner that is cost-efficient, essentially error-free, and respects individuals' rights and privacy.

This is being pursued in two major and mutually reinforcing ways. First, borders have been "pushed out" through the use of detailed passenger information provided by airlines that enable border officials to analyze it *before* individuals arrive at a port of entry (and, increasingly, even before they begin their travel). Second, new techniques are being employed to verify individuals' identity more effectively. Biometric information, such as fingerprints and retinal scans, is relied upon more routinely to complement traditional documents such as passports, which can be more easily obtained fraudulently or stolen. The use of biometrics also reflects a shift *away* from nationality as the dominant criterion for determining how much screening travelers undergo, focusing instead on individual characteristics. But the very authoritativeness and interoperable sharing of biometrics can also mean that unintentional errors based on these data — as well as deliberate fraud — are harder to undo.

The explosion in global travel and the dawning of the age of risk have exposed substantial weaknesses in border management systems.

These innovations, which have proliferated more widely in recent years, have not been without controversy. The growing reliance on personal information and characteristics in managing mobility has raised questions about data protection, privacy, and how individuals whose data have been misused — or accessed without authorization — can seek redress. As technologies to capture and verify individuals' identity and characteristics become more sophisticated, and increasingly interoperable systems allow information to be more easily shared, the "price" of making an error increases.

Diplomatic skirmishes during transatlantic negotiations reveal how sensitive these issues can be as countries try to negotiate international agreements on the use of personal data. Tensions between political actors within countries (or within the European Union) about the appropriate level and nature of protections add a layer of complexity to the discussions. Looking forward, consistent data-protection standards, including for contentious practices such as data mining and profiling, will not only assist international collaboration on security and mobility issues, but also help countries to consider national policies within a much more strategic framework, rather than relying on a patchwork of ad hoc agreements and practices.

International collaboration and partnerships play an increasingly critical role in border management, as the experience of the past decade shows. Visas, for instance, are not just a migration management tool but increasingly also a card on the table in foreign policy negotiations. In fact, advanced industrialized nations are embarking upon immigration and visa-related agreements with other nations with increasing frequency. The resulting complex of bilateral and multilateral pacts raises the question of whether there will be enough motivation for greater *global* coordination in the future. At the same time, advanced industrialized society must find ways to reach out to these other countries, such as the fast-emerging economies of Brazil, Russia, India, and China (BRIC), while recognizing and accepting policy differences — what is successful in one country may not work in another.

International collaboration and partnerships play an increasingly critical role in border management.

Governments and legislatures have been largely willing, so far, to dedicate enormous sums to building new border management systems. However, the benefits of new technology must be weighed against its costs *and limitations:* it requires enormous financial capital, is difficult to design and implement correctly, and rapidly becomes obsolete if it is not constantly updated to reflect evolving requirements. Despite huge investments, in fact, several projects have faltered due to serious design and implementation shortcomings. (This task is often in the hands of private contractors with substantial technical expertise but limited border management experience).The focus, then, must be on improving system knowledge (understanding travel flows, motivations, and practices) and analysis of data, while keeping in mind the long-term feasibility of a project. Governments thus need to allocate all forms of resources more strategically if this new border architecture is to grow and take its place as the principal means through which facilitation and security reach the equilibrium point that successful economies and societies demand — and have a right to expect.

I. Introduction

As global travel continues to grow, the sheer volume of border crossings — and diversification of points of entry — have put border management systems under constant pressure.[1] At the same time, additional risks associated with these movements have emerged, as devastating terrorist attacks, human trafficking, and growing unauthorized populations have exposed — and exploited — weaknesses in states' ability to manage their borders effectively. The response has been in many ways predictable. States have invested extraordinary amounts of physical, political, and diplomatic capital (both unilaterally and jointly) in reconceptualizing and implementing new border management frameworks. These frameworks seek to accomplish two almost equally crucial strategic aims: facilitating legitimate travel and trade (so that economies can continue to grow), while preventing the entry of would-be terrorists and criminals (and significantly reducing unauthorized immigrant entries).

This double imperative has fueled the search for and creation of new systems to allow border enforcement professionals to "preclear" the vast majority of travelers and cargo, and focus efforts on who or what is unknown and/or likely to be a threat. More importantly, the objective has become to allow these professionals to make these decisions as early as possible during an individual's (or a cargo's) travel, and as far from reaching a border as possible. This new architecture seeks to integrate several components into an integrated whole: new technologies, a much more elaborate information infrastructure (with real-time, interoperable databases), and much greater investments in new hardware and human resources. The long-term goal, which is much harder to accomplish, is to make facilitating mobility and security part of a single seamless management response.

[1] For example, the total number of international tourist arrivals worldwide increased from 69.3 million in 1960; to 165.8 million in 1970; to 278.1 million in 1980; to 439.5 million in 1990; and to 687 million in 2000. See Rey Koslowski, *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration* (Washington, DC: Migration Policy Institute, 2011).

Three major strategic shifts underpin this new architecture:

"Virtual" border control ("pushing out the borders") is now a full partner to territorial border control. New border management systems have taken advantage of technological developments to enhance the ability to identify people, assess risk, and share information before individuals reach and attempt to enter a country. (Clearly, land borders are well behind air and sea borders in that regard.) These investments have been costly, and raise new questions about privacy in the context of how data are collected, used, and exchanged.

Biometric data aim to replace nationality as a means of screening and identification. The increased use of detailed traveler information — including biometric identifiers — has raised questions about the continued centrality of nationality when assessing eligibility for entry into the destination country: indeed, citizenship is increasingly just one of a broader and ever-expanding set of individual characteristics and behaviors used to determine whether a person can travel to another country.

Governments have increasingly recognized the importance of international cooperation in securing more effective border management. This is not just in terms of exchanging data on travelers and potential threats, and maintaining virtual borders, but in managing physical borders. Partnerships with selected nongovernmental actors, especially in the private sector, are also increasingly prevalent.

Through partnership and information technology (IT) infrastructure, one might imagine that ports of entry and physical borders are on the way to becoming less important. However, as recent illegal migration flows across the Greek land border or continuing concerns about flows through the Mexico-US border highlight, technology and partnership maybe "merely" transforming the "fortress" model of border management into a "complex organism"[2] model, in which border security must fit together with other systems — both internally and internationally — to maintain the integrity of each state.[3]

This report outlines the key changes in border management over the past decade, highlights current and future challenges, and raises the following fundamental key question: what will be needed to ensure the successful operation of the new border management architecture?

II. Recent Innovations in Border Management

Over the past decade, states have invested enormously in new border management systems designed to achieve two potentially conflicting goals: facilitating mobility for legitimate travelers and impeding the mobility of those traveling without authorization or with maleficent intent. This challenge is compounded by several constraints, principal among them the need to ensure the privacy of the individual as far as possible.

The logistics of managing vast borders, multiple entry points, and an ever-increasing number of travelers — while maintaining the balance among security, mobility, and civil liberties — has put border management officials under unprecedented pressure. As a result, a number of major changes have taken place over the past decade. Some of these have been structured and planned reforms, while others have responded to specific events. Central to them all have been the technological advances

[2] The "fortress" metaphor refers to the hardening of external borders in an effort to restrict immigration and asylum policies for third-country nationals. The "complex organism" metaphor goes beyond looking at the border in isolation and looks at overlapping systems that work as an integrated whole to prevent unwanted migration while facilitating legitimate mobility.

[3] Chad C. Haddal, *People Crossing Borders: An Analysis of US Border Protection Policies* (Washington, DC: Congressional Research Service, 2010), www.fas.org/sgp/crs/homesec/R41237.pdf.

made available to those responsible for securing borders.

It is clear that the United States has invested deeply in technology to monitor entry into the country, though other immigration countries, above all Australia, have been thought leaders on how to attain the most effective border management. It is thus not surprising that the Australian entry-exit system (to monitor international travelers' arrival and departure) has become the standard for other major immigration regions to emulate, as the most advanced system of its kind. For the United States, the preoccupation with preventing another terrorist attack has led to a seemingly all-consuming pursuit of securing its borders by *all means available*.

European Union (EU) Member States, although newer to immigration, confront similar security concerns yet have been slower to move toward utilizing border technology,[4] in some part because several countries have nonexistent, or insubstantial, external borders. However, it should be noted that the European Union adds an additional complexity, and collaboration has been a major innovative feature of border management. The abolition of internal border controls within the EU Schengen area[5] has fueled the need for EU Member States to cooperate ever more closely to maintain the integrity of the European Union's *external* borders.[6] Thus European governments cooperate in the development of an EU system of integrated border management, while some continue to test and develop their own individual systems independently. While working closely together, Member States retain ultimate control of their own borders.

On a global level, the major border management innovations can be grouped into four main trends: collecting and sharing detailed traveler data, using new techniques to verify individuals' identity, employing new technology in monitoring physical borders, and building partnerships to achieve border management goals.

A. Collecting and Sharing Information

Governments are beginning to place greater emphasis on the need to collect data on people who wish to enter their country *before* their arrival at the border. The data collection ranges from biographical information contained in the passport (shared through Advance Passenger Information [API]), to more detailed information on travel plans (collected through Passenger Name Records [PNR]), and the purpose of an individual's visit (gleaned from visa applications). This information, historically collected through visa applications and at ports of entry, is no longer used just for immigration enforcement and the prevention of visa overstays, but also to assess potential security risks.

This new security focus is most evident in the United States. Following the terrorist attacks of 2001, the US government identified PNR[7] and API[8] as valuable sets of data from which they could draw information about individual travelers to match against watch lists and suspicious profiles. These are considered contentious due to the concerns over data protection, to which this report will return.

[4] Exceptions to this include the United Kingdom, the Netherlands, and Spain.

[5] The Schengen area involves 22 Member States of the European Union (except the United Kingdom, Ireland, Romania, Bulgaria, and Cyprus), as well as European Economic Area (EEA) partners Norway, Iceland, Switzerland, and Lichtenstein, and allows for freedom to move within this space for all travelers, regardless of citizenship.

[6] The European Union's external border is comprised of 42,672 kilometers (km) of sea borders and 8,826 km of land borders, involving 18 of the European Union's 22 Schengen states, and eight bordering non-EU States.

[7] The Passenger Name Record (PNR) is the generic name given to the files created by airlines for each journey booked by a passenger, which is stored in the airlines' reservation and departure control databases. PNR allows all the different agents within the air industry (from the travel agent and the computer reservation systems [CRS] to the carrier and the handling agents at the airports) to recognize each passenger and have access to all relevant information related to his/her journey, including departure and return flights, connecting flights, and special services required on board the flight.

[8] The Advance Passenger Information (API) system captures travelers' biographic data — information contained on the first page of a passport — during airline check-in and transmits it to border officials in advance of passengers' arrival into the country. The information can then be checked against computer databases and watch lists and used for immigration processing, security, and customs purposes. These systems are used to provide advance warning of persons of interest traveling to the country while quickly clearing low-risk passengers.

But these are not the only sources of information. The United States has developed numerous data-collection mechanisms at different points in the journey. For example, the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system collects biometric data (fingerprints and photographs) at the port of entry, while the Electronic System for Travel Authorization (ESTA)[9] checks individuals traveling via the Visa Waiver Program[10] against domestic watch lists (such as the "no-fly" list, and the terrorist watch list) before the journey begins. Much of the work of the last decade has been to improve the interoperability of these databases and ensure that all parts of the system communicate smoothly — and in real time —with one another. The other aim is to make progress toward "risk segmentation," an effort to designate threat assessments as early in the course of transit as possible. Both sets of processes have the goal of managing risk more effectively, which in turn makes facilitating mobility both more realistic and safer — and builds confidence in the ability of border agencies to protect the homeland.

> *Governments are beginning to place greater emphasis on the need to collect data on people who wish to enter their country* before *their arrival at the border.*

In the European context, the existence of Schengen ports of entry in multiple countries makes data sharing a necessary element of the collaboration, as it can help reduce the incidence of multiple or fraudulent visa applications. One of the earliest examples of this is the European Dactyloscopy (EURODAC), a centralized fingerprint database for all asylum seekers in the European Union, designed to reduce multiple asylum applications. It is clear also that, to date, the EU travel data-collection effort has been more concerned with immigration control than counterterrorism. For example, the European Union does not currently have an internal PNR agreement, and while current EU rules allow Member States to use API data, only a handful have enacted legislation to take advantage of this information source.

Considerable effort is also being made to ensure that related information systems in the different Member States (for example, each national visa information database) are capable of exchanging information with their counterparts. The most substantial development, to date, has been the effort to move from a basic alphanumeric Schengen Information System (SIS) (which collects information on visa refusals and other people of interest), to a biometric-based second-generation system (SIS II, projected to be operable by 2013). The technical work to establish this system forms the basis for other distinct collection efforts from the Visa Information System (VIS) (a database on all visa applications by third-country nationals entering the Schengen group), and proposed entry-exit and registered-traveler systems (which, in turn, are based on VIS information). Until SIS II and VIS are fully operable, however, the other initiatives will most likely remain on paper.

Who has access to data, and for what purpose they will be used, has been a major preoccupation of European policymakers. In practice, this has led to the development of stand-alone systems for each set of information, with limited and clearly defined rules of access and robust privacy protections. This preoccupation can be seen in the fact that the European Commission abandoned a proposal to allow law enforcement officials and Europol access to the EURODAC database in late 2010, anticipating opposition in the European Parliament, despite a call from a significant minority of Member States to extend this facility as soon as possible.[11] By contrast, US policymakers are more comfortable with

[9] The Electronic System for Travel Authorization (ESTA) is an automated system used to determine the eligibility of temporary visitors who would otherwise not be screened, that is, those traveling from visa waiver countries. ESTA adds a layer of security as it enables the US Department of Homeland Security (DHS) to analyze these individuals' biographic information before they begin their travel and thus determine whether they pose a threat or are otherwise ineligible to enter.

[10] The US Visa Waiver Program allows citizens of participating program countries to enter the US for up to 90 days without applying for a visa.

[11] European Commission, "On the establishment of 'EURODAC' (European Dactyloscopy) for the comparison of fingerprints for the effective application of Regulation (EC) No […/…] [establishing the criteria and mechanisms for determining the Member

broader access to databases, and are willing to develop additional functionality to address new goals. In effect, it is important to remain aware of the different contexts on both sides of the Atlantic. Europeans must appreciate the security priorities in the United States. The terrorist attacks of 9/11 permeate the thinking at all levels of government: the worst-case scenario for officials is another attack on domestic soil, therefore top priority is given to policies aimed at preventing anything similar from happening again.

Who has access to data, and for what purpose they will be used, has been a major preoccupation of European policymakers.

There are differences between how the European Union and the United States perceive agreements to exchange information across the Atlantic. In an effort to gather as much information as possible, the United States and Canada have negotiated agreements with the European Union itself, to allow for the transfer of critical information from airlines to government (PNR agreements), and access to partner government databases. Concerns that US authorities will use data for broader purposes — a so-called "mission creep" — have guided EU institutions toward cautious negotiation and, in the case of the European Parliament, open skepticism. A joint review of the EU-US PNR agreement outlined some European concerns about the expansive use of data in the United States, and responsiveness to ad hoc requests for information from other parts of the government.[12] These different approaches to data collection, and different perspectives on privacy, raise challenges with respect to how data are shared and exchanged across the Atlantic. The debate reopened once again in 2011, as the European Union and United States began negotiations not just on PNR, but on an overarching transatlantic data-protection agreement.

B. Verifying Information and Identity

Data collected on individual travelers is only as valuable as the accuracy of the information presented. The use of fraudulent identities is a continual weakness with respect to both immigration control and counterterrorism systems. As a result, most industrialized countries are adopting new methods for identifying travelers, primarily through biometric data, such as photographs, fingerprints, and retinal scans.[13] These data are matched with passport, visa, and passenger data to ensure that the name on the ticket matches the face presented.

Biometrics do not signify merely a shift to more sophisticated technology, they represent a larger shift toward the concept of identification through individual characteristics rather than on the basis of nationality. This is driven by the realization that home-grown terrorism exists in numerous "safe" countries, countries that cannot have wide-ranging visa restrictions placed upon all of their citizens. (Indeed, the ESTA program was intended to assuage concerns in the United States that visa waiver programs created security vulnerabilities.)

To compensate, some states also recognize that there are "safe" individuals, which has led to the

State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person](recast), COM(2010)555," October 11, 2010; Member States called for the Commission to reconsider access to EURODAC at a Justice and Home Affairs (JHA) Council meeting held on November 8, 2010.

[12] European Commission, *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS),* (Brussels: European Commission, 2010), www.dhs.gov/xlibrary/assets/privacy/privacy_eu_pnr_aircarriers_feb_2010.pdf.

[13] This is more developed in North America, with all non-US citizens fingerprinted upon entry. In Europe, provisions have been made for passports to contain biometric data via the incorporation of an electronic chip, though to date few countries have actually stored fingerprint and photograph data within the passport. Currently only EURODAC stores fingerprint information at the European level, though the SIS II database will also do so.

development of registered-traveler pilot programs, allowing privileged frequent travelers to fast track through security procedures.[14] These programs rely upon the ability to collect and compare biometric data, in order to quickly confirm identities. While such systems may hold great potential for border efficiency, they may also lead to a stratified approach to mobility, privileging those with means and access to technology.

With so much data collection and transfer, it is inevitable that mistakes will be made, with innocent individuals wrongly identified as threats. This is less of a problem when those individuals have the opportunity to have their case reviewed, and highlight possible errors. However, as Susan Ginsburg points out, the opportunities for non-US citizens to seek redress in the United States are more limited than they are for US citizens.[15] Indeed, access to redress becomes ever more crucial as databases multiply, and an error in one database migrates to and infects others. Sophisticated manipulation of data — such as mining[16] and profiling — may further compound this problem. It may be difficult for an individual to ensure redress in every part of the system, creating potentially Kafkaesque scenarios in which one's ability to travel becomes nearly impossible to restore. The US Department of Homeland Security's Traveler Redress Inquiry Program (TRIP) initiative, offering a one-stop shop for individuals to resolve travel screening problems, is a step in the right direction. It is clear, however, that a greater commitment is needed to allow individuals the opportunity to correct mistakes, perhaps by offering them greater access to the decision made and the reasoning behind it, as well as reliable interagency processes for ensuring that fixes are carried through the entire system.[17]

C. Monitoring Physical Borders with New Technology

For effective border management to take place, the integrity of physical borders is still critical. On both sides of the Atlantic, policymakers have taken several measures to ensure that fewer unauthorized border crossings occur.

Technology is used increasingly at the physical borders of industrialized countries. Tools such as seismic and infrared sensors, cameras, unmanned aerial vehicles, satellites, and radar coverage are designed to monitor borders and create a "virtual fence." In the United States, efforts to use technology at the border date back to the 1970s. The effort to create an integrated electronic border surveillance system, SBI*net*, proved too costly and problem-plagued and was terminated in January 2011 by the Obama administration; technology will continue to be deployed selectively based on geography and other criteria.[18] Across the Atlantic, Spain's Integrated System of External Vigilance (SIVE) detects boats making the journey from North Africa to Spanish shores.[19] With an eye to the apparent successes of this initiative, the European Union has proposed a European Border Surveillance System (EUROSUR) — a "system of systems" to facilitate the use of border technology. The framework is currently being studied by the European Commission with a view to proposing formal legislation in 2011.[20]

[14] Examples include the Netherlands' PRIVIUM program, NEXUS, and the Secure Electronic Network for Travelers Rapid Inspections (SENTRI) (between the United States and Canada, and United States and Mexico, respectively), the US Global Entry Program, and the United Kingdom's Iris Recognition Immigration System (IRIS) initiative.

[15] Susan Ginsburg, *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders* (Washington, DC: Migration Policy Institute, 2010): 252.

[16] Data mining is the process of identifying and extracting patterns from data, which can then be matched alongside profiles composed of characteristics and behavior deemed to be high-risk.

[17] Ginsburg, *Securing Human Mobility in the Age of Risk:* 260.

[18] Koslowski, *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration.*

[19] Jorgen Carling, *The Merits and Limitations of Spain's High-Tech Border Control* (Washington, DC: Migration Policy Institute), www.migrationinformation.org/USfocus/display.cfm?id=605.

[20] European Commission, *Examining the Creation of a European Border Surveillance System*, COM(2008) (Brussels: European Commission, 2008): 68.

In addition to using new methods of surveillance, governments are cooperating with neighboring countries to mitigate weak points in the systems. In North America, for instance, Canada and the United States cooperate deeply on border management with the introduction of Integrated Border Enforcement Teams (IBETs) that investigate instances of smuggling and illegal migration,[21] and a focus on increased coordination and information sharing to increase security. These developments fall under the umbrella of a Smart Border Action Plan, signed in 2001. A similar agreement was also signed with Mexico, though the extent of its implementation remains unclear.[22]

In the European Union, cooperation is more complex, due to the greater number of countries involved. Policymakers have been working toward an integrated system of border management, including a Common Border Code for all EU border officials and the establishment in 2005 of Frontex, an EU agency to oversee external border cooperation between Member States in the realm of border security. Given the constantly shifting pressure points at Europe's external borders,[23] and the uneven burden experienced by certain countries in southern Europe — first Spain, then Malta, Italy, and now Greece — the European Union has developed mechanisms to respond quickly in particular regions. Frontex has overseen a series of joint operations (several Member States joining together to patrol borders) in the Mediterranean, while the first deployment of the Rapid Border Intervention Teams (RABIT) — seconded teams of border officials from other EU countries — along the Greek land border was authorized in October 2010.[24]

D. *Building Partnerships*

Border hotspots shift according to the principle of least resistance: if surveillance is stepped up in one area, illegal migration flows move elsewhere. In the European context, some argue that the flows themselves remain fairly constant, diminished more by a perception of fewer job opportunities (such as during the recent recession and its aftermath) than direct border control. In an effort to prevent illegal migration before the point of border crossing, European governments and the European Union have invested in partnerships with key non-EU countries, particularly neighboring countries, such as that between Spain and Senegal, and between Italy and Libya.

Cooperation between countries on roughly equal levels of development is most advanced. Accordingly, partnership is most developed among EU Member States, and between the United States and Canada. Emerging cooperation can be identified on a transatlantic basis, but also through the Five Country Conference involving the United States, Canada, the United Kingdom, Australia, and New Zealand; and the Asia-Pacific Economic Cooperation (APEC), involving numerous Asian states, North America, and Latin America.

But external cooperation — that is to say, partnerships (of various forms) with less-industrialized countries — is crucial to effective border management. The United States engages in ever deeper cooperation with Mexico (and increasingly several Central American states) while the European Union has invested greatly in neighboring- and sending-state partnerships. These take many forms, from soft agreements such as mobility partnerships (with Moldova and Cape Verde), to legally binding readmission treaties (such as the newly agreed terms with Pakistan). In addition to formal agreements, the European Union spends a great deal of its available budget lines supporting the development of border management capacity in countries to the south and east. At the same time, individual Member States have engaged in bilateral agreements with third countries from which unauthorized migration flows are significant, or with whom they have historical ties. Examples include pacts between France and Morocco, and the more controversial agreement between Italy and Libya. There are no "typical"

[21] Chad C. Haddal, *Border Security: The Role of the U.S. Border Patrol* (Washington, DC: Congressional Research Service, 2010): 23, www.fas.org/sgp/crs/homesec/RL32562.pdf.
[22] See Appendix.
[23] See Christal Morehouse, *Irregular Migration in Europe* (Washington, DC: Migration Policy Institute, forthcoming 2011).
[24] Frontex, "Frontex deploys Rapid Border Intervention Teams to Greece," (press release, October 25, 2010), www.frontex.europa.eu/newsroom/news_releases/art79.html.

agreements, but mostly modest financial assistance is frequently offered in return for support in preventing the departure of unauthorized migrants to EU Member States, and accepting migrants found on EU territory (readmission agreements). In the case of Italy and Libya, the beginnings of cooperation go back over a decade but its depth — and effectiveness — have skyrocketed in the last two years despite concerns about the treatment of migrants in Libya, and has led to a broader EU-Libya dialogue on the issue.[25] Such agreements are frequently pursued on an informal level, given their sensitive nature.[26]

The objective of these partnerships from the EU side is primarily immigration control. However, while some are specifically focused on improving border surveillance, others also look more broadly at addressing push factors in sending countries. This can be most clearly seen in mobility partnerships, which include modest assistance for domestic employment development initiatives and agreements to facilitate *very limited* legal migration.

Clearly, many sending and transit countries to the south and east of Europe, such as Morocco or Tunisia, have less to gain from these partnerships and are thus reluctant to engage broadly with the European Union; others have few common interests in the area of migration and border cooperation.[27] This can be overcome through the use of financial support or through the broader framework of cooperation, offering greater opportunities for partnership with the European Union. Such broader framing can be seen in the Eastern Partnership Initiative, a 2008 repackaging of the European Neighborhood Policy, in which "mobility and security" was bundled in with issues such as energy security and promotion of trade.[28]

III. Emerging Challenges to the New Architecture

Many of these innovations have led to new patterns of international diplomacy and technology conundrums. As a result, it is not surprising that the path to a more elaborate, and complex, system of border architecture has created a number of challenges, particularly in respect to financial restraints, data usage, and fraud opportunities.

A. Costs and Infrastructure

Money dedicated to homeland security has almost been no object over the past decade, and investments in border management have increased correspondingly. Successive US administrations have doubled the number of border guards, for example, from 9,000 in 2001 to 20,000 in 2010.[29] Indeed, appropriations for border control over the last decade have increased by 235 percent, from $1.06 billion in fiscal year (FY) 2000 to $3.56 billion in FY 2011.[30] Similarly, the budget for Frontex in the European Union saw a fourteen-fold increase, albeit from a very small base number, from just 6.2 million euros in its first year of operation to 87.8 million euros in 2010. But as public budgets shrink in the aftermath of the global recession, the cost of developing and maintaining new infrastructure will come under greater scrutiny and require much more robust justification.

[25] For a detailed dissection of emerging bilateral relations between Italy and Libya, see Emanuela Paolotti and Ferruccio Pastore, *Sharing the dirty job on the southern front? Italian–Libyan relations on migration and their impact on the European Union* (Oxford, UK: IMI Working Paper, December 2010).

[26] Jean-Pierre Cassarino, *Readmission Policy in the European Union* (study for the European Parliament, 2010).

[27] Agnieszka Weinar, *Mobility Partnerships* (Washington, DC: Migration Policy Institute, forthcoming 2011).

[28] European Union, "Eastern Partnership" (press release, December 3, 2008), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/762.

[29] US Customs and Border Protection (CBP), "Snapshot" (fact sheet, July 2010). www.cbp.gov/linkhandler/cgov/about/accomplish/snapshot.ctt/snapshot.pdf.

[30] Haddal, *Border Security: The Role of the U.S. Border Patrol.*

Unexpected expense can arise at each step of the process, from the design and implementation of new systems to upgrade and maintenance, to new technology that complements existing architecture. Technology quickly becomes obsolete if not constantly updated to reflect changing threats and challenges. The flagship EU project to upgrade SIS illustrates how difficult these challenges can be. Originally scheduled to come online in 2007, the deadline has been pushed to 2013, due to both changing parameters and the complications inherent in integrating so many national systems. When work commenced in 2002, the system was expected to cost 15 million euros and hold up to 22 million traveler records. With the expansion of the Schengen area and increasing international mobility, the project has cost over 95 million euros over the past eight years (and may cost up to 143 million euros before it is operational) and will now need capacity for up to 100 million records. While Member States remain committed to the new Schengen system, in spring 2010 Germany and Austria publicly questioned the continued value of the project, expressing serious doubts as to whether the final system will achieve its original goals.[31]

The United States has experienced similar problems. For example, Homeland Security Secretary Janet Napolitano formally terminated the SBI*net* "virtual fence" program in January 2011, the finale to long-standing concerns regarding cost, deadlines, performance, and ultimate viability.[32] The US government had spent more than $1 billion on SBI*net* since 2006.[33] In canceling the program, Napolitano made clear that border enforcement would continue, with continued "boots on the ground" and more intensive "point defense" — deploying existing technology, such as surveillance drones, radar, and sensors, in strategic locations.[34,35]

Other projects confront more practical barriers to completion. The US-VISIT program was initially envisaged as an automated entry-exit system as far back as 1996, for example,[36] but implementing exit controls at both land and air borders has proved very difficult. Again, the goals of the entry-exit program changed over time as priorities shifted toward security concerns and new requirements were added (such as the introduction of biometric identifiers). While the value of the system is rarely questioned, it has cost around $350 million per fiscal year and these costs are set to continue for the foreseeable future, despite the fact that the "exit" portion of the system remains elusive.

But there are also signs of a move away from some of the newest technologies toward more "traditional" approaches, at least in the United States. In May 2010, President Obama announced the deployment of an additional 1,200 National Guard troops to the Southwest border.[37] This was followed by $600 million in supplemental funds provided by Congress for enhanced border protection and law enforcement activities, the lion's share going to bolster the number of Border Patrol agents and customs and immigration officers at official ports of entry, and just a small allocation for technology development. (In fact, the SBI*net* border surveillance program had its funding cut by $100 million in the same legislation.[38])

In some cases, the private sector has also borne some of the costs of increasing border security. Airlines, for example, have been asked to take on security responsibilities due to their unique position in mediating international travel. However, there are signs that companies may be becoming less willing to participate, as regulations require more active investments — such as longer periods of

[31] Austrian and German delegations, *Further Direction of SIS II,* Council of the European Union 10833/10, June 10, 2010, Brussels.

[32] US Government Accountability Office (GAO), *Border Security Fencing, Infrastructure and Technology (BSFIT) Fiscal Year 2010 Expenditure Plan,* Fiscal Year 2010 Report to Congress (Washington, DC: GAO, 2010)

[33] Ibid.

[34] Sharon Weinberger, "SBI*net* to be cancelled by Mid-November," AOL News, November 6, 2010.

[35] DHS, *Report on the Assessment of the Secure Border Initiative-Network (SBInet) Program* (Washington, DC: DHS, 2011), | www.globalsecurity.org/security/library/report/2011/sbi-net-assessment.pdf.

[36] *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*, section 110.a.1, "Automated Entry-Exit Control System," *US Congressional Record—House* (September 28, 1996): H11787.

[37] Michael D. Shear and Spencer S. Hsu, "President Obama to send more National Guard troops to US-Mexico border," *The Washington Post*, May 26, 2010. www.washingtonpost.com/wp-dyn/content/article/2010/05/25/AR2010052503227.html.

[38] Koslowski, *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration.*

data retention (which increases server cost) and the construction of infrastructure at the points of entry. Indeed, a recent US Government Accountability Office (GAO) evaluation of US-VISIT found that tests of exit controls at airports were not possible because no airline was willing to take part in the pilot program.[39] Other sectors, such as trucking and shipping, also incur the indirect costs of legal responsibility for unauthorized migrants found on board.

> *In some cases, the private sector has also borne some of the costs of increasing border security.*

Of course, border technology has also become a lucrative business for certain companies. The development of data collection and surveillance systems and forward-looking designs are all outsourced to corporations such as Symantec, Raytheon, Boeing, Oracle, and numerous consulting firms. The use of private contractors, not all of whom have experience in the field, brings its own challenges. Notably, failure to understand the complexities of border management can ultimately push costs up for government clients while undermining the value of the technologies implemented. The troubled SBI*net* program, for example, had more external consultants than agency officials working on it (especially Border Patrol officials), and concerns were raised from the outset as to the relative inexperience of the consortium of private-sector companies (led by Boeing) in the field of border control. In contrast, one of the most long-standing and effective databases used in the Canadian immigration system, the Computer Assisted Immigration Processing System (CAIPS), was actually designed by in-house immigration officials who may have had a stronger grasp of the more flexible needs of their fellow officials.[40]

To date, most budgets for developing border management systems have been reviewed in isolation, without a comprehensive approach to assessing which investments make most sense and how to distribute available funds. However, a more strategic approach to border spending will be important in future policymaking. In particular, policymakers will need to be sensitive to the fact that some technologies become obsolete quickly and some are particularly costly to maintain. These concerns will only intensify as budgets become more constrained.

B. *Data Usage and Efficacy*

The collection, use, and storage of data have expanded enormously, as described earlier. Defining and agreeing how these data should be used, and navigating the relationship between security and privacy objectives, remain central but unresolved challenges. Data have also dominated the critical transatlantic border management relationship. The central preoccupation of this debate has been about privacy and data protection. To date, many of the concerns have been expressed on the EU side, focusing on key issues such as redress, purpose limitation, and independent oversight.[41]

- ***Data-protection laws:*** While the European Union has a set of data-protection laws designed to ensure protection within the European Union,[42] it differs from the scope of the US 1974 Privacy Act (which only applies to US citizens and legal permanent residents).

[39] GAO, *Homeland Security: US-VISIT pilot evaluations offer limited understanding of air exit options* GAO-10-860 (Washington, DC, GAO, 2010), www.gao.gov/new.items/d10860.pdf.

[40] Conversation with Citizenship and Immigration Canada (CIC) official, July 27, 2010. The Computer Assisted Immigration Processing System (CAIPS) is in the process of being phased out and replaced by the Global Case Management System, which was designed by Public Works and Government Services Canada. See Treasury Board of Canada Secretariat, "Status Report on Major Crown Projects," www.tbs-sct.gc.ca/rpp/2008-2009/inst/imc/imc12-eng.asp.

[41] Paul De Hert and Rocco Bellanova, *Transatlantic Cooperation on Travelers' Data Processing* (Washington, DC: Migration Policy Institute, forthcoming 2011).

[42] European Commission Directive 95/46/EC supplemented by a 2008 Framework Decision on Data Protection.

- ***Data usage:*** Information can be used in different ways and for different purposes, and some uses are more controversial than others. Tensions have been highest in the case of data mining and profiling, creating links between different databases, and using information to identify individuals who have committed minor crimes (as opposed to terrorist plots or serious organized crime). In particular, the potential for data to be used for purposes other than tackling terrorism or serious crime and (where agreed) immigration management, continues to create concern.

- ***Wrongful identification and redress:*** With so much data collection and transfer, mistakes will inevitably be made, and innocent individuals wrongly identified as threats. This is less of a problem when those individuals have the opportunity to have their case reviewed, and highlight possible errors. However, in the US context, the opportunities for foreign citizens to have decisions reviewed are extremely limited. Indeed, access to redress becomes ever more crucial as databases multiply, repeating mistakes, and data mining further concretizes errors.

- ***Data retention:*** How long data are and can be kept differs within Europe and across the Atlantic. Some European countries, such as Germany and Austria, do not retain data beyond the initial inquiry, but others retain information for many years, and the United States for as long as 15 years.[43] Long data retention periods exacerbate concerns about the nature and accuracy of the data retained, and the purpose for which it is used.

- ***Onward transfer of data:*** Concerns remain that data will be passed on once more to third countries with less strict data-protection laws. These concerns highlight the fact that information, once shared, is no longer "owned" and joins other flows of information streaming into the larger databases in the partner country, much as tributaries join a river.

The lack of an overarching EU-US agreement on privacy and data protection remains the key hurdle for transatlantic cooperation and an obstacle to expanding the scope of data sharing. It also implies a patchwork of bilateral agreements between the United States and individual Member States, often with review and renewal clauses. This can leave little time to discuss other mobility-related issues such as visa policies, exit controls, and third-country support.[44]

Until very recently, it was thought that most issues related to data protection were resolved in a 2008 EU-US High Level Contact Group (HLCG), convened to negotiate a set of nonbinding common principles on information sharing, privacy, and personal data protection to smooth the way for future exchanges. However, recent documents from the European Commission throw this assumption into question. On the one hand, the Commissioner for Justice, Fundamental Rights, and Citizenship, Viviane Reding, has published a draft mandate for negotiating an overarching EU-US data-protection agreement, which would address all agreements related to data transfers in the investigation of serious crime and terrorism. While the mandate draws from the HLCG, it states that the European Union is not bound by it in negotiations, sets a number of additional limits on data use and processing, and highlights the question of access to redress.[45] Meanwhile, the Commissioner for Home Affairs, Cecilia Malmström, has issued guidelines for specifically negotiating simultaneous passenger data agreements with the United States, Canada, and Australia.[46]

The European Union's effort to clarify its terms of engagement is a useful starting point for the latest round of transatlantic PNR negotiations, even if it is not sufficient to ensure compatibility. Behind this, however, lies the broader question of how much data collection and usage is enough. Is the absence of

[43] Peter Hobbing, "The tools called to support the 'delivery' of Freedom Security and Justice: A comparison of border security systems in the EU and the US" (Briefing paper, Policy Department C: Citizen's Rights and Constitutional Affairs, European Parliament, Brussels, 2009), www.ceps.eu/system/files/old/ToolsEP.pdf.

[44] Ginsburg, *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders.*

[45] European Commission, *Recommendation to the Council to open negotiations for an agreement between the EU and the US on protection of personal data* (Brussels: European Commission, 2010).

[46] European Commission, *On the global approach to transfers of passenger name record (PNR) data to third countries* COM(2010)492 (Brussels, September 2010).

a major terrorist incident in the transatlantic space over the past five years itself a sufficient rationale for the continuing widespread collection of data? Are all of the data collected necessary, and which are the most useful? Data were critical to the capture of Faisal Shahzad, the perpetrator of the attempted May 2010 car bombing in New York City, for example,[47] and policymakers claim that 15 of the 19 perpetrators of the Sept. 11, 2001 attacks could have been caught with the use of PNR data. But data collection alone cannot prevent terrorist attacks, and effective screening will continue to rely heavily on sufficient manpower and more traditional forms of intelligence.

One way in which governments have attempted to be more proactive in identifying threats is to use data mining and profiling. PNR data, in particular, have opened up a new landscape for identifying potential travelers of interest for further scrutiny. Data mining is considered controversial even within the national security context, however. Security experts and civil liberties groups alike have raised concerns about who should be allowed to process the information (especially in cases in which this is outsourced to private software firms), and about the accuracy of data and the quality of the analysis, given the torrent of information and the very small number and diverse background of terrorist profiles on which analysts can base their statistical models. Furthermore, while data mining can expose patterns and relationships, it cannot describe causal factors or highlight the particular value of these patterns.[48] It is, in effect, a blunt instrument for a sensitive policy area.

One way in which governments have attempted to be more proactive in identifying threats is to use data mining and profiling.

With data collection now an established element of border management, it is timely to undertake an evaluation of its methods, purposes, and efficacy. Addressing some of the concerns that have arisen from data processing, and offering greater clarity about how policies balance data protection and the flow of information to border and security officials, will be important for maintaining public trust in border management.

C. *Identity Fraud*

Substantial investments have been made in verifying individuals' identity and detecting potential wrongdoers. However, integrated systems can also confirm (and proliferate) cases of mistaken identity. These cases may involve individuals wrongly identified as threats, as discussed earlier, as well as individuals who have fraudulently obtained another identity.

Despite the strong focus on identifying individuals at the earliest opportunity through travel documents and personal information, less focus is placed on how those travel documents are obtained. Of particular importance is the security of breeder documents,[49] such as birth certificates and social security cards, through which passports and identity cards are issued. Once a document (such as a passport or national ID card) is issued, biometric data often anchors the individual to that document. This offers stronger security in the case of an authentic identity, but may also cement and legitimize a fraudulently obtained passport. Thus, in the age of biometrics, breeder documents have become more, rather than less, relevant to border security and management.

In the United States, breeder documents are issued at the state or local level: there are 16,000 different offices that can issue birth certificates, and over 14,000 different kinds of birth certificates.[50]

[47] Janet Napolitano, "Securing the Skies: A Global Push for Aviation Security," *Foreign Affairs*, August 2, 2010, www.foreignaffairs.com/articles/66505/janet-napolitano/securing-the-skies?page=show.

[48] Jeffrey W. Seifert, *Data Mining and Homeland Security: An Overview* (Washington, DC: Congressional Research Service, 2008), http://assets.opencrs.com/rpts/RL31798_20080827.pdf.

[49] This is discussed in greater detail in Ginsburg, *Securing Human Mobility,* chapter 7.

[50] Ibid.

There are no common requirements and little consistency among them, and thus such documents are highly susceptible to forgery. In addition, it is particularly easy to submit genuine documents and assume the identity thereon; most passport fraud in the United States occurs this way. A GAO investigation has highlighted how easy it is to obtain a passport even with fairly obvious application discrepancies.[51]

In the European Union, national identity cards are common, and tend to require relatively rigorous cross-referencing of documents. This is partly because ID cards can now be used when traveling within the Schengen area in lieu of a passport. However, Member States have a broad range of different rules on the documents required to obtain passports. In an effort to address this, the European Union has issued a resolution authorizing further investigation as to how breeder documents can be brought into line.[52]

Beyond the transatlantic space, the challenge grows larger. If North American and European countries struggle to ensure the integrity of passports, then how can they be sure of the integrity of documents used to obtain passports in third countries? In an effort to manage this issue with major sending countries, the European Union has made the security of breeder documents an element in the roadmap to visa facilitation agreements. Leveraging visa opportunities on a bilateral basis, however, is a time-consuming method of improving document security.

IV. Considerations for the Future

A. *National System Design*

The use of information technology has been the most obvious transformation in border management over the past decade. Some critics, however, have highlighted that the exponential growth of IT systems in border management has failed to fully take into account such issues as proportionality of cost, infrastructure, and use, while suffering from the overarching problem of "equating information with knowledge."[53] Future policy developments will need to be sensitive to this risk.

First, policymakers face the challenge of ensuring that the ever-evolving potential of IT systems does not obscure critical weaknesses such as the vulnerability of breeder documents or the continuing need to allocate resources to more traditional elements of border management (i.e. border physical infrastructure and staffing). Ensuring a good fit among physical border control infrastructure, human resources, and information technology will remain important — especially given the fact that some technologies become obsolete quickly and upgrading them on an ongoing basis will be expensive.

Second, border management developments must operate within the strict parameters of a legal framework. The philosophy behind technological advancement is to push the boundaries of interoperability and function as far as imagination and technological capability can take them. But, as EU Member States are now debating, just because something is possible does not mean it should be done.

[51] GAO, *State Department: Undercover tests show passport issuance process remains vulnerable to fraud* GAO-10-922T (Washington, DC: GAO, 2010), www.gao.gov/products/GAO-10-922T.

[52] European Commission, "Position of the European Parliament adopted at first reading on 14 January 2009 with a view to the adoption of Regulation (EC) No .../2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States," (Brussels: European Commission, 2009), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:046E:0127:0127:EN:PDF.

[53] Peter Shields, "ICTs and the European Union's Evolving Border Surveillance Architecture: A Critical Assessment," *Observatorio Journal*, 4 (1), 255-88. www.obercom.pt/ojs/index.php/obs/article/view/331/349.

Third, private-sector contractors will always be integral to border technology development, but reliance on them raises some tricky questions. In addition to enduring concerns about whether private contractors can be sufficiently attuned to the needs of border protection officers on the ground, some skeptics have argued that the confluence of security companies' profit motives and political pressures on governments has led to an inflation of ambition and overestimation of both desirability and feasibility of new technologies.[54] The close relationship that has necessarily developed between technology companies and policymakers — exemplified by groupings such as the European Security Research and Innovation Forum, established by the European Commission, or the many US firms that service the multibillion-dollar needs of the Department of Homeland Security (DHS) — means there are few disinterested analysts capable of objectively considering the merits of a proposed innovation or design, and emerging problems are discovered too late.

Constantly shifting on-the-ground realities and priorities compound the difficulties in ensuring that final systems are still relevant and usable for those who manage borders; experience demonstrates that closer cooperation is critical. A good example is one of the most long-standing and effective databases used in the Canadian immigration system, the Computer Assisted Immigration Processing System (CAIPS). It was designed by in-house immigration officials with a strong grasp of the needs of their fellow officials.[55]

Border management developments must operate within the strict parameters of a legal framework.

How can policymakers work more effectively with their contractors to ensure problems are flagged and dealt with in a timely fashion? Efforts to address these problems in the European Union have included an emphasis on bringing critical IT expertise in-house and an agreement to establish an agency to oversee large-scale IT systems. Concerns about an overly cozy collaboration between government officials and corporate executives on both sides of the Atlantic may also be addressed with strong input from independent experts. These experts can help policymakers improve transparency and accountability, as well as flag problems before they become critical. While the oversight of the European Data Protection Supervisor (an independent adjudicator of data protection) has built in a critical review mechanism on the EU side, it is clear that nongovernmental observers lack both timely access to information and the opportunities to put forward their concerns.

B. *The Transatlantic Partnership: Ensuring Cooperation*

Differences in transatlantic approaches to data collection and usage, and to the protections afforded to individuals (both citizens and noncitizens), are likely to endure for some time. Differences across the Atlantic are not insurmountable, as previous successful PNR negotiations attest. But the process to find common ground has now become more complex. In particular, efforts by the EU-US High Level Working Group to find common principles for data sharing have now been thrown into question by the two mandates published by the EU Commissioner for Fundamental Rights and Commissioner for Home Affairs.

In addition to any philosophical and/or practical differences between EU and US policymakers, a delicate political balance *within* the European Union and United States also complicates the process of reaching agreement. On the European side, not only do common positions rely on the collective agreement of many different countries, but the advent of the Lisbon Treaty has introduced

[54] See for example, Peter Burgess and Monica Hansen, " Private Dialogue in Security Research," (Briefing paper, European Parliament LIBE Committee, 2008); Didier Bigo and Julien Jeandesboz, "The EU and the European Security Industry: Questioning the 'public-private dialogue'," (INEX policy brief no. 5, Centre for European Policy Studies, 2010), www.ceps.eu/book/eu-and-european-security-industry-questioning-%E2%80%98public-private-dialogue%E2%80%99.

[55] E-mail exchange with CIC official, November 12, 2010.

a new actor — the European Parliament — which now has a critical role in the negotiation of data-sharing agreements. However irascible US officials may have found some Member States up to now, the European Parliament has historically adopted a more aggressive stance regarding protection of individual rights. In 2010, the European Parliament proved a tough partner regarding bank data transfers (rejecting the first version of the Society for Worldwide Interbank Financial Telecommunications [SWIFT] agreement), and is unlikely to prove as accommodating as previous negotiating partners.[56]

In the United States, the executive branch must accommodate the views of Congress, which has often championed extensive border security measures and was the source of additional restrictions, such as the conditions placed on visa waiver programs in 2007, including ESTA. In other words, both EU and US positions must take into account the constraints created by internal political actors that can reduce the room for maneuver: what may look like a unilateral imposition may actually be the result of a hard-fought domestic political compromise.

Looking forward, a set of binding overarching common principles and a workable negotiating mechanism will be needed. In the absence of structured dialogue, the ad hoc approach that has been followed to date will become ever more time-consuming, and the battle to renew and forge additional agreements will be fought on the same territory time and time again. Efforts to create an overarching EU-US data-protection instrument need to be prioritized by both parties, and include all political actors in negotiations from the outset. Despite the challenge of developing overarching principles, this process would offer both Europeans and North Americans an opportunity to objectively review and evaluate their legislation and domestic structures for border management and data exchange.

Not all calls for reform come from outsiders. Voices within the US government, such as GAO, have called for strengthened privacy laws and independent oversight of data use, while the European Data Protection Supervisor has been deeply critical of recent EU proposals. Thus the adoption of a common framework of principle and practice should be seen as an opportunity to invest in internal reform as well as a step forward in transatlantic diplomacy.

The transatlantic partnership also offers opportunities for mutual learning. The European Union is currently considering a number of initiatives that have already been implemented (or at least attempted) in the United States, such as an entry-exit system, registered-traveler systems, and surveillance technology. Indeed, the European Commission has commissioned an 'impact assessment' of how an entry-exit system might work in Europe; one hopes this draws upon the US-VISIT experiences to inform the Commission's forthcoming proposal. While the political dialogue on transatlantic border management garners the most attention, strong partnerships are also being forged at the technical and operational levels that will be key to future success.

Finally, the establishment of common principles and a solid working relationship across the Atlantic can form a foundation and become the driver for other cooperation in other regions and countries.

C. *A Global System of Border Management?*

International cooperation on border management over the last decade has occurred largely on an ad hoc basis, through bilateral talks, opportunistic deal making, or rules that place obligations on third parties. The proliferation of bilateral and multilateral partnerships among sending, transit, and receiving countries has created a dazzling complexity of rules and standards. The time has come for a more coherent approach to collaboration, even beyond the transatlantic relationship.

Currently, the system of international travel revolves around the issuance of visas modulated by bilateral

[56] European Parliament, Press Release, “Swift II: Civil Liberties Committee approves draft agreement,” (press release, May 7, 2010), www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20100705IPR77848+0+DOC+PDF+V0//EN.

and multilateral agreements between states. Visa systems authorize travel on the basis of individual assessments made at consulates, but also allow exceptions according to nationality. While the rules on visa issuance have traditionally focused on immigration controls, visas also play an increasing role in foreign policy. In the European Union, for example, the possibility of visa waiver or visa facilitation has dominated partnership discussions with non-EU countries. In recent EU-Russia dialogue talks, Moscow (and certain Member States) emphasized the need for visa-free travel, and foreign policy was also instrumental in the recent decision to offer Albania and Bosnia visa-free access to the European Union. And in the United States, the North American Free Trade Agreement (NAFTA) and free trade agreements with Chile, Australia, and Singapore, have created preferential access to temporary work visas for the highly skilled.

International cooperation on border management over the last decade has occurred largely on an ad hoc basis.

The events of September 11, 2001, and subsequent terrorist attacks have brought about dramatic changes in international travel. Increasingly, individual characteristics have become much more relevant in determining the ability to travel and rights of entry to sovereign states. For example, one can argue that the ESTA program has weakened the significance of the visa waiver for partner-country travelers, just as registered-traveler programs highlight how individual data can be also used to confirm low-risk travelers. The introduction of biometric identifiers has made the idea of an entirely new system of global travel based on individual profiles, rather than visa applications, more viable. This is not necessarily a welcome development for all countries. Those unable to afford the technical infrastructure for biometric identification, as well as those who use visas as a political tool, may lose more than they gain if leading receiving countries emphasize individual identification.

V. Conclusion

The dual role of nationality and individual characteristics is likely to endure for the foreseeable future as governments implement new border management systems while exploring the potential for greater bilateral and regional collaboration. To date, industrialized countries eager to forge workable partnerships on a bilateral or regional basis have faced formidable difficulties, suggesting that establishing a global system of border management would be an enormous challenge. However, the impetus for coherent global standards, interoperable systems, or even a global approach to border security could grow as more actors are affected by the border policies of groupings of states. Global businesses, for example, have a strong interest in facilitating mobility and reducing the complexity and regulatory burden of changing border management systems. And more generally, the coherence of international border systems has implications for the business of travel, openness, and ultimately, economic growth.

Drawing from the observations and analysis so far, as well as emerging patterns, policymakers should consider the following recommendations to improve border management systems:

> ***Reduce incompatible and ad hoc policy development.*** A key element to doing so is to adopt a whole-of-system approach, not just in terms of coordination but to ensure that policies complement each other. If border management is becoming a "complex organism," policymakers should consider how each element fits within it.

Balance goals and consider tradeoffs. While massive investments have been made in securing identities and ever stronger border controls, it is necessary to look at these investments in the context of the overall policy objectives of preventing terrorist attacks and controlling illegal immigration (both of which have an international *and* a domestic dimension). These objectives must dovetail with facilitating the mobility that is the lifeline of open societies and vibrant economies.

Feasibility and desirability must go together. Technological innovation has provided a wealth of potential solutions that simultaneously ensure the safety of citizens and the facilitation of international mobility. However, given the legacy infrastructures already in place, the changing goals and priorities of policymakers, the realities on-the-ground personnel face, the very likely limitations on new resources, and the lead time advanced technologies require, policymakers must keep the long-term feasibility of a project in mind throughout the development process.

Improve knowledge always. Fixing a problem in one area along a border does not necessarily solve it; all too often it simply shifts the problem to elsewhere in the system. Understanding traveler flows, motivations, and practices is invaluable to officials hoping to reduce the volume of illegal entries. Similarly, mapping and addressing weak points in the system — such as the fraudulent use of *breeder* documents — is fundamental. A border system will only be as strong as its weakest point.

Analysis is as important as collection. With torrents of information arriving in transatlantic databases every day, it is critical that there are sufficient resources to judiciously assess and draw out key pieces of intelligence. Blind reliance on data mining and profiling without the finer distinctions that distinguish good-risk from bad-risk data-management algorithms, may only serve to blur an already vague picture of who is a threat at any given time.

Context is key. In the minds of many governments on both sides of the Atlantic, the ultimate border management tool is the entry-exit system used in Australia. However, as the United States understands, the particular geography of the Antipodes— specifically, the absence of land borders of entry — is critical to that system's success. When learning from each other, the European Union and North America should keep in mind not just the historical evolution of policy choices, but also geography, the nature of migration flows, *and relations with neighboring countries*. What works in one context may not work in another.

Partnerships are instrumental. While advanced industrial societies already give priority to their mutual relationships, they must find ways to include other countries (such as important economic partners in their neighborhood, BRIC countries, and other emerging economies) in the discussion. Given the importance of human mobility to economies, it is critical that countries find a way to work together to find mechanisms that ensures individual travel even when particular governments may not "play ball."

Continuous monitoring and evaluation. The ad hoc development and constant evolution of many of these systems and their incremental intrusions into the scope of privacy and personal rights suggest that independent monitoring and evaluation must be augmented. In addition, the at-times dysfunctional and all too often opaque and disturbingly "cozy" relationships between government officials and private contractors suggest that independent technical and policy evaluation is needed, not just at the outset of a project, but throughout the process of implementation. Citizen advisory panels, supported by technical experts as needed, could offer a good way forward for addressing the more troubling aspects of such systems.

International guidelines. The twin goals of ensuring security and mobility are too important to leave to a hodge-podge of bilateral compromises. Agreement on a set of guidelines that address privacy concerns, establish necessary safeguards, ensure that systems work together efficiently, and allow travelers to rely on a transparent set of rules has already become necessary. Given the current EU-US discussions, it is time to draw out clearly commonalities and lines in the sand. The International Civil Aviation Organization may be well placed to be asked to build on the work it has already achieved in the area of document standardization and its nonbinding guidelines on data protection.

Underlying the urgency of acting now is the realization that unilateral acts by one country or bloc may ultimately prove to be shortsighted and costly. Governments require a good understanding of the various laws and technological capabilities that exist in partner countries. More importantly, they must understand and respect the privacy and security trade-offs each country has made when developing its own border management systems. Decisions taken by democratic governments in this area are not only politically sensitive, more importantly, they speak to the relationship between a citizenry and its government, a relationship which is itself a product of history and the evolution of a society.

Finally, the human dimension of border management will always remain central. In this sense, policymakers should ensure that technological capability is a function of policy and political choice, rather than its determinant, and seek to balance security objectives with respect for individual liberties and the facilitation of mobility.

For more on the Transatlantic Council on Migration, please visit:
www.migrationpolicy.org/transatlantic

Appendix: Canada, EU, and US Border Management Initiatives since 1995

CANADA			
INITIATIVE / DATE ENACTED	FUNCTION	NOTES	CORRELATING SYSTEMS
Partners in Protection (PIP) (1995)	Commitment to voluntary high security standards for commercial operators in order to create "trusted traders."	In 2009, the US and Canadian governments announced a plan to integrate PIP and Customs-Trade Partnership Against Terrorism (C-TPAT).	US[a] – Customs-Trade Partnership Against Terrorism (C-TPAT) (see below). Asia-Pacific Economic Cooperation (APEC), Taiwan, Australia, the Netherlands, Sweden, United Kingdom, European Union[b] – Authorized Economic Operator. Singapore[c] – Secure Trade Partnership. New Zealand[d] – Secure Exports Scheme.
Integrated Border Enforcement Teams (IBET) (1996)	Multi-agency law enforcement team consisting of both Canadian and American members seeking to investigate and control smuggling, terror threats, and illegal migration; devoted to information sharing.	Began in 1996 as a joint project between British Columbia and Washington state; has since gradually expanded across the US-Canada border.	European Union - Rapid Border Intervention Teams, made up of pooled nationality border guards responding to areas of need (see below).
Joint facilities ("one-stop" or "single-window" border crossings) (2000)	To increase efficiency and decrease costs by building shared border facilities.	Enacted by the Smart Border Action Plan (see below) in 2001.	European Union[e] - Joint facilities have existed at select checkpoints since the 1960s. APEC[f] – Single-window implementation in progress. Southeast European Cooperative Initiative[g] – currently introducing joint facilities among EU and non-EU neighbors. South and East Africa[h]– select crossings open; identified as a crucial policy action. Commonwealth of Independent States[i] – working toward joint facilities and customs unions; Belarus and Russia share single-stop facilities.
Smart Border Action Plan (2001)	A 32-point plan to build a "21st century" border system that respects both national security and economic objectives.	Impetus for many initiatives below.	US/Mexico – Similar plan agreed in principle in 2002.
Advanced Passenger Information/ Passenger Name Record (API/ PNR) (US, 2001; EU-Swiss, 2006)	Information provided by airlines prior to passenger entry to Canada. API = personal data (i.e. date of birth, gender). PNR = travel data (i.e. ticket information).	Canada-US agreement to share this information.[j] Canada-EU[k] and Canada-Swiss[l] agreements.	European Union – internal and external sharing agreements currently in place, but being reconsidered. United States – prefers to seek bilateral agreements (i.e. with the Czech Republic)[m], particularly as agreement with European Union is in dispute.

NEXUS (2002)	Expedited border crossing for preapproved travelers.	Jointly administered by Canada Border Services Agency (CBSA)/US Customs and Border Protection (CBP); CANPASS[n] was Canadian predecessor, made redundant by NEXUS unless individual is unable to qualify for express entry into the United States.	US/Mexico- SENTRI between United States and Mexico (see below).
Free and Secure Trade (FAST) (2003)	Commercial clearance and expedited border-crossing program.	Joint CBP/CBSA initiative; one of US Trusted Traveler programs; must be in PIP in order to qualify for FAST.	Mexico[o] – FAST is also in operation along the US-Mexico border.
Canadian Border Services Agency (CBSA)'s Arming Initiative (2006)	Arming Canadian border patrol officers; eliminating work-alone situations.	Two-year implementation program.	United States - CBP agents armed and have been since inception. European Union[p] – Varies among nations and internal/external borders.
Border Information Flow Architecture (2006)	Funding program that aims to enable an "effective interaction of technologies."	Partnership with the US Federal Highway Administration.	European Union - European External Border Surveillance System (EUROSUR) proposal (see below).
Advance Commercial Information (ACI) (Phase 1, 2004; Phase 2, 2006)	To provide CBSA officers with electronic, prearrival information about cargo.	Phase 1 required cargo information 24 hours before a marine vessel left foreign port; Phase 2 expanded marine requirements to the United States, and required all air shipments to send information four hours prior to arrival.	United States - Container Security Initiative (CSI) (see below)
eManifest (2009)	See above.	Phase 3 of ACI; expanded to cargo, conveyances, crew/passengers, and exporter/importer information entering through highway and rail border crossings.	See above.
Five Country Conference (FCC) High Value Data Sharing Protocol (2009)	Biometric (primarily fingerprint) sharing program for management of immigration and refugee/asylum systems.	Canada, United States, Australia, United Kingdom participating; New Zealand considering.[q] Privacy concerns voiced in many countries.	European Union - European Dactyloscopy (EURODAC) for asylum seekers and refugees.
Canada-US Action Plan for Critical Infrastructure (2010)	Designed to protect critical infrastructure between the two countries through increased risk management and information sharing.	Set specific milestones through 2013.	United States[r] - 1998 Presidential Decision Directive PDD-63 for the creation of a national critical infrastructure program. European Union[s] - EUCOMM 786 (2006) European Programme for Critical Infrastructure Protection.

EUROPEAN UNION

INITIATIVE / DATE ENACTED	FUNCTION	NOTES	CORRELATING SYSTEMS
Schengen Information System (SIS) (1995)	An information exchange system allowing border and judicial officials to obtain information on persons and objects.	Created through the Schengen Convention in 1995, eventually to be replaced by SIS II. Currently alphanumeric only.	
European Dactyloscopy (EURODAC) (2000)	Fingerprint database, to help identify asylum applicants and persons apprehended in connection with an irregular crossing of an external border of the European Union.	Recent proposals to allow law enforcement access to the database have recently been dropped by the European Commission.	
Advanced Passenger Information (API) (2004)	Biographical information taken from the machine-readable part of a passport and communicated by airline carriers to border control authorities.	Agreed by Directive 2004/82/EC of August 29, 2004 on the obligation of carriers to communicate passenger data. All EU States can use it, but few have done so to date.	Australia, Canada, India, Mexico, South Korea, Spain, and the United Kingdom have all enacted legislation requiring API.[t]
Integrated Border Management Agency (FRONTEX) (2005)	Agency to support external border cooperation within the European Union.	Proposals for the expansion of FRONTEX's mandate currently under discussion	
Schengen Borders Code (2006)	Common rules for the management of EU external borders.	Frequently revised, most recently revisions to the Borders Code (on long-stay visas) in April 2010.	
PNR agreements (Canada,[u] 2006 (exp.); US,[v] 2007; Australia,[w] 2008)	Agreements to transfer information provided by passengers and collected by carriers for enabling reservations.	The European Commission has recently published guidelines for PNR agreements, and will open simultaneous negotiations for new agreements with the United States and Canada.[x] The European Parliament will be involved in these negotiations also. Currently there is no EU-wide legislation allowing for use of PNR data for law enforcement, though a number of Member States have legislation enabling this use. The United Kingdom already has a functioning PNR system.	Canada/Australia/United States – similar PNR agreements are in place on a bilateral basis.
Rapid Border Intervention Teams (RABIT) (2007)	Teams of national experts providing technical and operational assistance in response to a Member State request. Coordinated by FRONTEX.	A RABIT team deployed for the first time in late 2010 along the Greek land border. Up to 600 officials from Member States can be called upon to join the team.[y]	United States/Canada – IBET teams (see above).

Visa Information System (VIS) – forthcoming (2010 exp.)	A system enabling the exchange of information on visa issuance and refusal between Member States. Access will be granted to designated authorities of Member States and by Europol for the purposes of the prevention, detection, and investigation of terrorist offenses or other serious crime.	Established through the Council Decision 2004/512/EC of June 8, 2004, and dependent on migration from SIS to SIS II.	
2nd Generation Schengen Information System (SIS II) – forthcoming (2013 exp.)	Upgrade of original SIS to cope with larger number of entries, and include biometric data.	Has been a long, controversial upgrade, with revised technical parameters, deadlines, and budget forecasts. Now expected to be online in 2013, after extensive testing in 2012.[z]	
Agency for the operational management of large-scale IT systems in the area of freedom, security, and justice – forthcoming (Agreed 2010)	This would establish a single management structure for SIS II, VIS, EURODAC, and other large-scale IT systems in the EU Justice and Home Affairs (JHA) area.	Proposed in 2009, it has a provisional agreement, though no set implementation date.	
European External Border Surveillance System (EUROSUR) – no formal proposal, not agreed[aa] (No date)	A "system of systems" to enhance cooperation between Member States' existing surveillance systems, and facilitate use of state-of-the-art technology to monitor borders.	Currently the European Commission is undertaking feasibility studies, and reporting back to the Council.[bb] A legislative proposal is expected in 2011.	
Registered-Traveler System – no formal proposal, not agreed[cc] (no date)	System for offering simplified, automated border checks for travelers who meet certain criteria.	Dependent on the implementation of VIS.	NEXUS, PRIVIUM, Etc.
Entry-exit system for third-country nationals – no formal proposal, not agreed[dd] (no date)	Information system to facilitate identification of 'overstayers' at earliest opportunity.	Dependent on the implementation of VIS.	US-VISIT
EU Electronic Travel Authorization System – no formal proposal, not agreed[ee] (no date)	Identification database for third-country nationals traveling on visa waiver programs	Dependent on the implementation of VIS.	US ESTA

UNITED STATES			
INITIATIVE / DATE ENACTED	**FUNCTION**	**NOTES**	**CORRELATING SYSTEMS**
Secure Electronic Network for Travelers Rapid Inspection (SENTRI) (1995)	Expedited CBP processing for preapproved, low-risk travelers.	Focused on land border traffic at the US-Mexico border, primarily in California, Texas, and Arizona.	United States-Canada – similar to NEXUS program in place (see above).
Smart Border Action Plan (Mexico) (2002)	A 22-point US-Mexico plan to harmonize point-of-entry operations, combat unauthorized immigrant smuggling, and improve screening of third-country nationals.	Agreed in principle, little evidence of direct implementation.	United States-Canada – similar plan outlined above.

Container Security Initiative (CSI) (2002)	Prescreening of commercial containers before they depart foreign ports.	The program has exceeded its goal of pre-screening 85 percent of all US-bound cargo.	Canada – Advance Commercial Information.
United States Visitor and Immigrant Status Indicator Technology (US-VISIT) (2003)	US-VISIT is a Department of Homeland Security (DHS) system for collecting biometric data, accessible to federal, state, and local agencies. Photographs and ten-digit fingerprints are collected from visitors and used for security/anti-terrorism purposes.	Originally only for those travelers requiring a visa, but since 2004 has been expanded to the Visa Waiver Program (VWP) and US lawful permanent residents. Most Canadians are not subject to US-VISIT.	Brazil[ff] – requested an exemption and when denied, implemented a program of photographing and fingerprinting American visitors Japan[gg] – J-VIS. South Korea[hh] – Fingerprinting foreign visitors.
Global Entry (2003)	An expedited CBP clearance program consolidating various registered-traveler systems – NEXUS (Canada), SENTRI (Mexico), and FAST (North America); applicable also for those holding a machine-readable UK passport, a green card or a US passport.		Germany[ii] – Automated Biometrics-Supported Border Controls.
SBI*net* (2006; canceled January 2011)	A digital network for the integration of infrastructure, personnel, and technology along both the northern and southern borders. Goal was to predict, prevent, deter, and respond to illegal activity. Includes communications and surveillance equipment, computer analysis, and rapid response teams.	Mandated as part of the Secure Borders Initiative (SBI). Was terminated in January 2011 by the Obama administration, amid technology issues, concerns about cost, and congressional criticism.	
US-EU PNR Agreement (2004, 2007)	European Union agrees to allow US access to PNR from European commercial carriers.	EU Parliament looking to renegotiate 2007 agreement and harmonize PNR agreements with other countries;[jj] United States seeks bilateral agreements with individual European states (i.e. the Czech Republic).[kk]	Canada, Australia – both have bilateral PNR agreements with the European Union.
Electronic System for Travel Authorization (ESTA) (2007)	Predeparture authorization required of VWP travelers, in the form of an online I-94W. Enacted in response to Congress' efforts to revoke the VWP, due to security concerns.	Information used by DHS, the Census Bureau, and the Department of Commerce.	Australia[ll] – Electronic Travel Authority.
FLUX (2009)	Partnership between US citizen portion of Global Entry and the Netherlands' Privium program.	Grants expedited entry into Schengen area.	

[a] US Customs and Border Protection (CBP), "C-TPAT: Customs-Trade Partnership Against Terrorism," www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/.

[b] Asia-Pacific Economic Cooperation (APEC), "Authorized Economic Operator Compendium," (2010) http://aimp.apec.org/Documents/2010/SCCP/SCCP2/10_sccp2_015.pdf; Taiwan Council for Economic Planning and Development, "Authorized Economic

Operators Offered Customs Facilitation," (2010) www.cepd.gov.tw/encontent/m1.aspx?sNo=0013131; Australian Customs and Border Protection Service, "Authorized Economic Operator Pilot Project Report," (2009) www.customs.gov.au/webdata/resources/files/AEO_Report.pdf; Dutch Customs Administration (Douane), "Authorized Economic Operator," www.douane.nl/zakelijk/aeo/en/;
Swedish Customs Service (Tullverket), "Authorized Economic Operator," www.tullverket.se/en/startpage/keywordsaz/az/authorisedeconomicoperatoraeo.4.2337793011afcaba766800010.html; HM Customs & Revenue, "Authorized Economic Operator (AEO) scheme," (2007) http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageImport_ShowContent&propertyType=document&id=HMCE_PROD1_028236; European Commission: Taxation and Customs Union, "Authorized Economic Operator (AEO)," (2010) http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/aeo/index_en.htm.

[c] Singapore Customs, "Secure Trade Partnership (STP)," (2011) www.customs.gov.sg/leftNav/trad/Supply+Chain+Security.htm.

[d] New Zealand Customs Service, "Secure Exports Scheme," www.customs.govt.nz/exporters/Secure+Exports+Scheme.htm.

[e] For information on one-stop borders internationally, see Erich Kieck, "Coordinated border management: unlocking trade opportunities through one stop border posts," *World Customs Journal* 4, no. 1 (2010): 3-13. www.worldcustomsjournal.org/media/wcj/-2010/1/Kieck.pdf.

[f] APEC, "Authorized Economic Operator Compendium," (2010) http://aimp.apec.org/Documents/2010/SCCP/SCCP2/10_sccp2_015.pdf.

[g] Southeast European Cooperative Initiative, "Infrastructure – Border Crossing Facilitation," www.secinet.info/index.php?option=com_content&view=article&id=165&Itemid=81&showall=1.

[h] Department for International Development, "Trade boosts as one stop border post opens," (December 8, 2009) http://webarchive.nationalarchives.gov.uk/+/http://www.dfid.gov.uk/Media-Room/News-Stories/2009/One-stop-border-post-opens/; USAID: East Africa, "One Stop Border Post Helps Streamline Transit Times," (August 28, 2007) http://eastafrica.usaid.gov/en/Article.1074.aspx; USAID, "One Stop Border Posts Facilitate Transport," www.satradehub.org/index.php?option=com_content&task=view&id=120&Itemid=519.

[i] Central Asia Regional Economic Cooperation, "Regional Trade Facilitation and Customs Cooperation Program In Support of Joint Transport and Trade Facilitation Strategy," (2008) www.carecinstitute.org/uploads/events/2008/7th-MC/CAREC-TFCCC-report.pdf.

[j] Canada Border Services Agency (CBSA), "Advance Passenger Information/Passenger Name Record," (2008) www.cbsa-asfc.gc.ca/media/facts-faits/004-eng.html.

[k] *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 Record data," (2006) www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_eng.pdf.

[l] Swiss Federal Administration News, "Memorandum of Understanding Between the Canada Border Services Agency and the Swiss Federal Office for Civil Aviation Concerning Advance Passenger Information/Passenger Name Record," www.news.admin.ch/NSBSubscriber/message/attachments/2242.pdf.

[m] Statewatch, "Memorandum of understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America regarding the Unites States Visa Waiver Program and related enhanced security measures," (2008) www.statewatch.org/news/2008/mar/us-czech-mou-visas-etc.pdf.

[n] CBSA, "CANPASS," www.cbsa-asfc.gc.ca/prog/canpass/menu-eng.html.

[o] US Department of Homeland Security (DHS), "Free and Secure Trade (FAST) Implementation on the US/Mexico Border," (2003) www.dhs.gov/xnews/releases/press_release_0309.shtm.

[p] Frontex, "Frontex training unit," www.frontex.europa.eu/structure/capacity_building_division/training/.

[q] UK Border Agency, "Checking migrants' fingerprints," www.ukba.homeoffice.gov.uk/managing3/borders/checking-fingerprints/.

[r] Federation of American Scientists, "Presidential Decision Directive/NSC-63: Critical Infrastructure Protection," (May 22, 1998). www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[s] Commission of the European Communities, "Communication from the Commission on a European Programme for Critical Infrastructure Protection," (2006) http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

[t] SITA, "Spain's APIS Border Control System: Technical brief," (2010) www.sita.aero/file/4828/Spain_APIS-border_control_system_technical_brief.pdf.

[u] European Commission: Home Affairs, "Agreement between the EU and Canada on Passenger Name Record data" http://ec.europa.eu/home-affairs/policies/police/police_pnr_canada_en.htm.

[v] European Commission: Home Affairs, "Agreement between the EU and US on Passenger Name Record data," http://ec.europa.eu/home-affairs/policies/police/police_pnr_us_en.htm.

[w] European Commission: Home Affairs, "Agreement between the EU and Australia on Passenger Name Record data," http://ec.europa.eu/home-affairs/policies/police/police_pnr_australia_en.htm.

[x] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, "On the global approach to transfers of Passenger Name Record (PNR) data to third countries," COM(2010)492 (21 September 2010). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0492:FIN:EN:HTML.

[y] Frontex, "Frontex deploys Rapid Border Intervention Teams to Greece," (October 25, 2010) www.frontex.europa.eu/newsroom/news_releases/art79.html.

[z] Council of the European Union, "Council conclusions on SIS II," (October 2010) www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/116946.pdf.

[aa] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Examining the creation of a European border surveillance system (EUROSUR)," COM(2008) 68 (13 February 2008) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0068:FIN:EN:HTML.

[bb] Commission of the European Communities, "Commission Staff Working Paper: Report on Progress Made in Developing The European Border Surveillance System (EUROSUR)," (24 September 2009) http://ec.europa.eu/home-affairs/doc_centre/borders/docs/sec_2009_1265_en.pdf.

[cc] 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 (13 February 2008) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0069:FIN:EN:HTML.

[dd] Ibid.

[ee] Ibid.

[ff] BBC News, "Brazil to fingerprint US citizens," (December 31, 2003) http://news.bbc.co.uk/2/hi/americas/3358627.stm.

[gg] Japanese Ministry of Justice and Immigration Bureau, "New entry procedures will start," (English instructional poster) www.immi-moj.go.jp/keiziban/happyou/pdf/poster-english.pdf.

[hh] BBC News, "South Korea introduces fingerprint scans for suspicious foreign visitors," (September 6, 2010) www.telegraph.co.uk/expat/expatnews/7977361/South-Korea-introduces-fingerprint-scans-for-suspicious-foreign-visitors.html.

[ii] Bundespolizei, "Automated and Biometrics-Supported Border Controls (ABG) at Frankfurt Airport," www.bundespolizei.de/cln_152/nn_719704/EN/Home/AutomatedBorderControls/abc__node.html?__nnn=true.

[jj] European Parliament, "European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada,"www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN&language=EN.

[kk] Statewatch, "Memorandum of understanding between the Ministry of the Interior of the Czech Republic and the Department of Homeland Security of the United States of America regarding the Unites States Visa Waiver Program and related enhanced security measures," (2008) www.statewatch.org/news/2008/mar/us-czech-mou-visas-etc.pdf.

[ll] Australian Department of Immigration and Citizenship, "Electronic Travel Authority (ETA) – Online Applications," www.immi.gov.au/e_visa/eta.htm.

All sites accessed February 2011.

Works Cited

Austrian and German delegations. 2010. *Further Direction of SIS II10833/10.* Brussels: Council of the European Union.

Bigo, Didier and Julien Jeandesboz. 2010. *The EU and the European Security Industry: questioning the 'public-private dialogue*. Brussels: Centre for European Policy Studies. www.ceps.eu/node/2999.

Burgess, Peter and Monica Hanssen. 2008. *Public-Private Dialogue in Security Research*, PE 393.286. Brussels: European Parliament.

Carling, Jorgen. 2007. *The Merits and Limitations of Spain's High-Tech Border Control.* Washington, DC: Migration Policy Institute. www.migrationinformation.org/USfocus/display.cfm?id=605.

Cassarino, Jean-Pierre. 2010. *Readmission Policy in the European Union*. Luxembourg: European Parliament.

Citizenship and Immigration Canada (CIC). 2008. Status Report on Major Crown Projects Global Case Management System. Ottawa: CIC. www.tbs-sct.gc.ca/rpp/2008-2009/inst/imc/imc12-eng.asp.

De Hert, Paul and Rocco Bellanova. Forthcoming. *Transatlantic Cooperation on Travelers' Data Processing*. Washington, DC: Migration Policy Institute.

Department of Homeland Security (DHS). 2011. *Report on the Assessment of the Secure Border Initiative-Network (SBInet) Program*. Washington, DC: DHS. www.globalsecurity.org/security/library/report/2011/sbi-net-assessment.pdf.

Europa. 2008. Eastern Partnership. News release, December 3, 2008. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/762.

European Commission. 2008. *Examining the Creation of a European Border Surveillance System,* COM (2008) 68. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0068:FIN:EN:HTML.

_____. 2010. On the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person](recast), COM(2010)555. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010PC0555:EN:HTML.

_____. 2010. *Report on the joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS)*. www.dhs.gov/xlibrary/assets/privacy/privacy_eu_pnr_aircarriers_feb_2010.pdf.

_____. 2010. On the global approach to transfers of passenger name record (PNR) data to third countries, COM(2010) 492. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/COMM_NATIVE_COM_2010_0492_F_EN_COMMUNICATION.pdf.

European Parliament. 2010. European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2010-0144+0+DOC+XML+V0//EN.

_____. 2010. SWIFT II: Civil Liberties Committee approves draft agreement. News release, July 5, 2010. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+IM-PRESS+20100705IPR77848+0+DOC+PDF+V0//EN.

European Parliament and European Council. 2009. Position of the European Parliament adopted at first reading on 14 January 2009, with a view to the adoption of Regulation (EC) No .../2009 of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:046E:0127:0127:EN:PDF.

Frontex. 2010. Frontex deploys Rapid Border Intervention Teams to Greece. News release, October 25, 2010. www.frontex.europa.eu/newsroom/news_releases/art79.html.

Ginsburg, Susan. 2010. *Securing Human Mobility in the Age of Risk: New Challenges for Travel, Migration, and Borders*. Washington, DC: Migration Policy Institute.

Haddal, Chad C. 2010. *Border Security: The Role of the U.S. Border Patrol*. Washington, DC: Congressional Research Service. www.fas.org/sgp/crs/homesec/RL32562.pdf.

______. 2010. *People Crossing Borders: An Analysis of U.S. Border Protection Policies*. Washington, DC. Congressional Research Service. www.fas.org/sgp/crs/homesec/R41237.pdf.

Hobbing, Peter. 2009. The tools called to support the 'delivery' of Freedom Security and Justice: A comparison of border security systems in the EU and the US. Briefing Paper, Policy Department C: Citizen's Rights and Constitutional Affairs. Brussels: European Parliament.

Koslowski, Rey. 2011. *The Evolution of Border Controls as a Mechanism to Prevent Illegal Immigration*. Washington, DC: Migration Policy Institute.

Morehouse, Christal. 2011 forthcoming. *Irregular Migration in Europe*. Washington, DC: Migration Policy Institute.

Napolitano, Janet. 2010. Securing the Skies: A Global Push for Aviation Security. *Foreign Affairs*, August 2, 2010. www.foreignaffairs.com/articles/66505/janet-napolitano/securing-the-skies?page=show.

Paolotti, Emanuela and Ferruccio Pastore. 2010. Sharing the dirty job on the southern front? Italian–Libyan relations on migration and their impact on the European Union. Oxford, UK: IMI Working Paper.

Seifert, Jeffrey W. 2008. *Data Mining and Homeland Security: An Overview*. Washington, DC: Congressional Research Service. http://assets.opencrs.com/rpts/RL31798_20080827.pdf.

Shear, Michael and Spencer S. Hsu. 2010. President Obama to send more National Guard troops to US-Mexico border. *The Washington Post*, May 26, 2010. www.washingtonpost.com/wp-dyn/content/article/2010/05/25/AR2010052503227.html.

Shields, Peter. 2010. ICTs and the European Union's Evolving Border Surveillance Architecture: A critical Assessment. *Observatorio Journal* 4 (1): 255-88.

US Customs and Border Protection (CBP). 2010. Snapshot. Washington, DC: CBP. www.cbp.gov/linkhandler/cgov/about/accomplish/snapshot.ctt/snapshot.pdf.

US Government Accountability Office (GAO). 2010. *Border Security Fencing, Infrastructure and Technology (BSFIT) Fiscal Year 2010 Expenditure Plan*, GAO-10-877R. Washington, DC: GAO. www.gao.gov/new.items/d10877r.pdf.

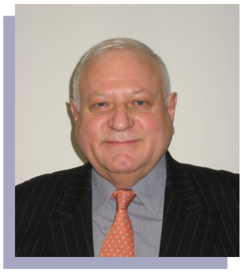
______. 2010. *Homeland Security: US-VISIT pilot evaluations offer limited understanding of air exit option*, GAO-10-860. Washington, DC: GAO. www.gao.gov/new.items/d10860.pdf.

______. 2010. *State Department: Undercover tests show passport issuance process remains vulnerable to fraud*, GAO-10-922. www.gao.gov/new.items/d10922t.pdf.

Weinar, Agnieszka. 2011 forthcoming. *Mobility Partnerships*. Washington, DC: Migration Policy Institute.

Weinberger, Sharon. 2010. SBI-net to be cancelled by Mid-November. AOL News, November 6, 2010.

About the Authors



Demetrios G. Papademetriou is President and Co-Founder of the Migration Policy Institute (MPI), a Washington-based think tank dedicated exclusively to the study of international migration. He is also the convener of the Transatlantic Council on Migration and its predecessor, the Transatlantic Task Force on Immigration and Integration (co-convened with the Bertelsmann Stiftung). Dr. Papademetriou is also Co-Founder and International Chair Emeritus of *Metropolis: An International Forum for Research and Policy on Migration and Cities*. He is Chair of the World Economic Forum's Global Agenda Council on Migration.

Dr. Papademetriou holds a PhD in Comparative Public Policy and International Relations (1976) and has taught at the universities of Maryland, Duke, American, and New School for Social Research.

He has held a wide range of senior positions that include: Chair of the Migration Committee of the Paris-based Organization for Economic Cooperation and Development (OECD); Director for Immigration Policy and Research at the US Department of Labor and Chair of the Secretary of Labor's Immigration Policy Task Force; and Executive Editor of the *International Migration Review.*

Dr. Papademetriou has published more than 250 books, articles, monographs, and research reports on migration topics and advises senior government and political party officials in more than 20 countries, including numerous European Union (EU) Member States while they hold the rotating EU presidency.

Elizabeth Collett is a European Policy Fellow at the Migration Policy Institute and Senior Advisor to MPI's Transatlantic Council on Migration. She is based in Brussels and works on the International Program, with a particular focus on European policy.

Prior to joining MPI, Ms. Collett was a Senior Policy Analyst at the European Policy Centre (EPC), an independent Brussels-based think tank, and responsible for its migration program, which covered all aspects of European migration and integration policy. During her time at EPC, she produced numerous working papers and policy briefs focused on the future of European Union immigration policy. She has also worked in the Migration Research and Policy Department of the International Organization for Migration in Geneva and for the Institute for the Study of International Migration in Washington, DC.

Ms. Collett holds a Master's degree in Foreign Service (with Distinction) from Georgetown University, where she specialized in foreign policy and earned a certificate in refugee and humanitarian studies, and a Bachelor's degree in law from Oxford University.

mpi
MIGRATION POLICY INSTITUTE

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

www.migrationpolicy.org

1400 16th Street NW
Suite 300
Washington, DC 20036

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