The European Union has proposed new comprehensive travel security measures, including the introduction of biometric-data identifiers for any visitor entering the EU. The new proposals are meant to streamline border-crossing procedures and data-collecting processes on an EU-wide basis. But the United States is still insisting on striking bilateral deals with individual nations, undermining what some European leaders say should be a multinational procedure.

Both the US and the EU are moving toward biometrically enabled travel documents and new proposals for border controls meant to combine greater security and more convenience to legitimate travelers. However, the impasse over how the US will extend its Visa Waiver Program (VWP) might indicate a looming policy incompatibility.

Officials worldwide appear to be pursuing the same goals for safe travel. However, different regimes are moving forward with different technologies and procedures at different rates. Many times, a government’s stated reasons for wanting more information from its citizens doesn’t match the citizens’ motivations for accepting the new technology.

On the surface, similar goals

“In today’s interconnected world, facilitating travel between partner nations with a common focus on security is not only beneficial—it’s imperative,” US Secretary of Homeland Security Michael Chertoff said in signing VWP agreements with Hungary, Slovakia, and Lithuania on 17 March. “We’re fortunate to have strong ties with each of these countries, and with the European Union. As we move forward with other aspiring allies toward visa-free travel, we will also continue to collaborate with the European Union, especially in areas where it has unique legal authority.”

The three bilateral deals were signed just days after the US rebuffed EU’s attempt to reach a blocwide deal. US and EU negotiators issued a terse joint statement after a 13 March meeting failed to establish an EU-wide VWP agreement. The statement mentioned agreement only that “in the process of concluding Memoranda of Understanding and implementing arrangements concerning the Visa Waiver Programme, a twin track approach would be followed. Those matters that fall within national responsibilities will be discussed with national authorities while those that fall within EU responsibility will be discussed with EU authorities.” The statement didn’t elaborate on these delineations of responsibility.

At the same conference, the US agreed to conclude discussions with the EU regarding implementation of its Electronic System for Travel Authorization by June (www.eu2008.si/en/News_and_Documents/Press_Releases/March/0313JHA_EU_ZDA_Statement.html).

While awaiting the ESTA specifics, privacy advocates and advocates of a European community-based approach to international travel have criticized the nations that signed deals with the US and the EU’s own enhanced security blueprint.
"A common visa policy is a community competence," said Urszula Gacek, the European parliament member speaking for EPP-ED, the legislative body’s Christian Democrat and European membership. "Furthermore, member states are obliged to adhere to the principle of solidarity in this area. If this principle has been undermined, it is necessary to consider why. Those bodies that have the competence to deal with this matter should do so effectively. Those who are obliged to show solidarity in this area should not ignore this requirement.

"The EU needs a concrete timetable which would give real hope for finding a speedy solution to the problem, and the EPP-ED Group wishes to assure the Commission that it will support it in achieving the aim of equal rights to visa-free tourist travel for all EU citizens.”

The ongoing impasse is particularly vexing for Europeans, who reluctantly agreed to more stringent US-backed Passenger Name Records for air travelers in 2007. The final agreement took the place of one stricken by the European Court of Justice as not adhering to EU privacy protections.

Yet the new EU travel proposals include stipulations that privacy advocates also see as onerous.

“The EU has picked up the torch and is running with ill-considered policies on border surveillance,” Gus Hosein, project director of Privacy International’s Terrorism and the Open Society Program, wrote in a commentary in The Guardian (http://commentisfree.guardian.co.uk/gus_hosein/2008/02/sky_spies.html) after the EU plan was announced in February. “And it will succeed. Not only because the EU decision-making processes in security affairs lack accountability. Not just because the EU has been complicit in US travel surveillance programmes for years. But because the prevailing mood in the UK and across Europe is to call for ‘tougher borders’ without quite knowing what that means.”

A patchwork in the making
Since the terror attacks of 11 September 2001, officials worldwide have reached basic consensus on more stringent requirements for travel documents. The technology underlying biometric travel documents is widely standardized under the auspices of the International Civil Aviation Organization (www.icao.int). ICAO approved the facial recognition standard in 2003, and first-generation passports implementing it in chips using RFID technology are now standard issue in many nations.

The US, for example, has been exclusively issuing what the State Department calls the e-passport since August 2007. In addition to the old-style passport’s human-readable photograph, the e-passport contains a digital image of the photograph to facilitate the use of face-recognition technology at ports of entry, a unique chip identification number, and a digital signature to protect the stored data from alteration.

Even though the US is widely considered to be the driving force behind collecting more and more personal data from travelers, other nations are already issuing biometric passports with technologies that go beyond digital photos. For example, since 1 November 2007, Germany has mandated that citizens applying for passports supply two fingerprints as well as a photo. According to the German Ministry of the Interior, the prints are taken using a scanner at the passport authority when the application is submitted. When the finger is pressed against the scanner’s glass plate, it’s captured electronically within seconds. As a rule, both index fingers are scanned three times in a row. The software instantly and automatically chooses the best sample. If necessary, the system can sample other fingers as well. The passport application process will take only slightly longer than it did before fingerprint scanning was introduced.

The technological differences in the US and German passports illustrate the gulf between different regime policies as well. Paradoxically, the US is widely perceived to be the most concerned about the prospect of terrorists slipping into the country because of inadequate identification procedures, yet it has opted to make advanced biometric technology an optional aspect of travel documents instead of a government mandate as the Germans have.
The US advanced biometric program is a public/private partnership called Registered Traveler (RT), operated under the auspices of the Department of Homeland Security’s Transportation Safety Administration. However, private contractors actually perform the program’s operations. Currently, the TSA has approved eight vendors to participate (www.tsa.gov/approach/rt/vendors.shtm).

The RT program (www.tsa.gov/approach/rt/index.shtm) uses advanced biometrics (iris scans or fingerprinting) and a TSA Security Threat Assessment background check based on an applicant’s answers to a questionnaire. Those who pass the background check are then issued a TSA-approved card containing the biometric data, which is used in conjunction with—not instead of—an approved photo ID document, for a fee above and beyond the fee for a government-issued passport. The identity on a participating traveler’s card is checked against data residing in the program’s Central Identity Management System, operated by the American Association of Airport Executives’ Transportation Security Clearinghouse. The program lets enrolled travelers bypass the regular security line at participating airports. Instead, these travelers can go through the RT line. Vendors claim that RTs can spend 30 percent less time waiting for security checks. In addition, international travelers should be able to participate in RT by 2010, according to legislation signed by US president George W. Bush on 27 December 2007.

The EU’s biometrically based proposal, announced on 13 February (http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/85&format=HTML&aged=0&language=en&guiLanguage=en#fn8), also calls for an RT program, but the EU’s vice president for justice, Franco Frattini, called for only reliable travel history (that is, no overstays in other countries), proof of subsistence, and a biometric passport in setting the program’s parameters. In addition, Frattini proposed requiring EU-bound travelers who don’t enjoy visa waivers to also provide biometric facial images and fingerprints for inclusion in the EU’s Visa Information System. He expects to be fully online by 2012.

Verified Identity Pass, a vendor for a voluntary US identity credentialing programs, said the company welcomes Frattini’s new ideas. “We’re in conversations now with US and non-US government agencies and private companies about partnerships,” a company spokesperson said. “And we believe the public/private partnership that we work within on the US Registered Traveler program should be viewed as a model to work within here—allowing the government agencies to do what they do best and the private companies do what they do best so that the partnership is optimally structured.”

**Ambiguity and opposition**

Civil libertarian advocates claim the registered traveler programs encroach on the principles of a democratic society. The American Civil Liberties Union, for example, cited the fuzzy information available about what exactly constitutes a security assessment threat, whether those who are rejected for RT status will have the right of redress, and the creation of economic disparities between those who can afford to pay for enhanced biometric security and clearance status and those who can’t. (TSA representatives did not respond to an interview request.)

Perhaps the most scientific exploration of global acceptance of biometrics is “Biometrics and e-identity (e-passport) in the European Union: end-user perspectives on the adoption of a controversial innovation,” published in the *Journal of Theoretical and Applied Electronic Commerce Research* by researchers from the University of South Australia, University of Koblenz-Landau, and New York University (www.uni-koblenz.de/~iwi/publications/ag-hampe/NgkSwaHamReb_2005_Biometrics_CollECTeR-Europe.pdf). The study’s authors found that acceptance of biometric identity technologies varied greatly by country, often depending on the country’s general level of technology adoption. They also discovered that different nations placed different emphasis on the perceived motivation for using biometric documents. Overall, for example, 64 percent of study respondents believed e-passports would better protect the user from document forgery, and only 48 percent believed it would protect a nation from terrorists. However, respondents from the United Kingdom and Spain, the two nations most aligned with the US in fighting terrorism, recorded scores of 59 and 60 percent, respectively, in assessing the e-passport as an anti-terror tool.
Overall, the authors reported that 57 percent of the study’s respondents were positive about e-passports and just 13 percent were negative about them. This overall acceptance rate, especially considering the newness of the technology and the ongoing policy disputes between jurisdictions, worries advocates such as Privacy International’s Hosein.

“We don’t seem to mind border surveillance because we always imagine it applies to someone else,” he warned in his Guardian essay. “But there is nowhere in the world that you are more powerless than at the border of another country. You are at the whim of any government official’s mood or interest. Worse yet, you’re at the whim of technology that will never quite work the way it is promised to you by governments (if they bother to tell you).”

Cite this article: