The Privacy Office
Homeland Security

Privacy Matters

Chief Privacy Officer's Message

It is my privilege to serve as the Acting Chief Privacy Officer for the Department of Homeland Security. I thank my predecessor, Nuala O'Connor Kelly, for her vision and leadership. During her tenure, the Privacy Office accomplished a great deal, becoming a privacy leader throughout the Federal government.

As we move forward, our mission and our resolve are renewed. We are building upon the foundation we have laid, continuing our work with our DHS colleagues, the Data Privacy and Integrity Advisory Committee, citizens groups and the private sector. We are adding staff, increasing expertise, and promoting four critical goals: continuing to provide department-wide privacy guidance, rolling out new department-wide privacy education and training programs, leading the development of privacy protections within information-sharing environments, and continuing to strengthen our relationships with our international partners to promote security through cross-border collaboration.

Thank you for your continuing support of the Privacy Office. We look forward to working with you in pursuing privacy safeguards while enhancing the security of our nation.

-Maureen Cooney, Acting Chief Privacy Officer

Inside This Issue, Winter 2006

Privacy Office Holds First Public Workshop

Explores Government Use of Commercial Data for Homeland Security

On September 8 and 9, 2005, the Department of Homeland Security (DHS) Privacy Office hosted its first public workshop, "Privacy and Technology: Exploring Government Use of Commercial Data for Homeland Security." The objective of the workshop was to look at the policy, legal, and technology issues associated with the government's use of commercial personally identifiable data in homeland security. A broad range of experts, including representatives from government, academia, and business participated in the panel discussions. At the end of each panel, the audience was given an opportunity to address questions to the panelists.

The workshop opened with a panel discussion of how government agencies are using commercial data to aid in homeland security. Representatives from government agencies that use commercial data, as well as commercial data providers, discussed the many ways the data is used including verification, profiling, and pattern matching. The panel discussed the ease and accuracy of using commercial data, suggesting that due to the ease with which data can be

See WORKSHOP, page 2

Data Privacy and Integrity Advisory Committee:

On the web at,

www.dhs.gov/privacy

On email at,

privacycommittee@dhs.gov

First Joint Review of PNR Undertakings A Success

U.S.— EU Joint Review Highlights Cross-Border Information Sharing Effort

WASHINGTON, DC— On September 20 and 21, 2005, delegations from the U.S. Department of Homeland Security (DHS) and the European Commission performed the first Joint Review of the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) concerning Passenger Name Record (PNR) information derived from flights between the U.S. and the European Union (EU). Prior to the Joint Review, the DHS Privacy Office conducted an internal review of CBP policies, procedures and technical implementation related to the data covered by the Undertakings.

U.S. and EU review teams, led by Nuala O'Connor Kelly, Chief Privacy Officer of DHS and Francisco Fonseca Morillo, Director, Commission Directorate General Justice, Freedom and Security, engaged in two days of review and site visits. The teams were comprised of officials from border and transportation, data protection, and law enforcement, including representatives from EU Member States and senior CBP officials. The review considered the implementation of the PNR Undertakings by CBP, and through site visits to CBP operations at Dulles Airport and the National Targeting Center, the teams learned more about how PNR data is used to facilitate travel into and out of the U.S. and screen for individuals or groups related to terrorism or transnational crimes. The two teams were able to engage in a thorough

See U.S./EU, page 2

Privacy Office Workshop Continued

obtained, appropriate measures should be taken to protect the privacy and security of the information.

The next panel addressed the legal issues raised by the government's use of commercial data. The panelists discussed the Privacy Act of 1974, which provides the fundamental privacy protections that govern personal information held by the federal government. The panelists were largely in agreement regarding the many exceptions that agencies are allowed to elect and the enforcement mechanism in place, intimating that the protection in the Act may be diminished with respect to addressing modern uses of commercial data. The panelists suggested that, rather than looking to amend the Act, ways to strengthen compliance through the development of sound privacy guidance should be explored.

The first day ended with a panel on the current and developing technologies that can aid the government in data analysis. Panelists explained that at its core, information technology can provide a force-multiplier to the ability to draw meaning from raw data. Data that would otherwise seem random and disconnected may be brought together and made meaningful through the use of technology. Choosing the right technology for the right purpose with the right discrete functionality, however, is crucial. The panel discussed the types of analytical tools available and what they can and cannot do.

The second day began with a discussion on how technology can help protect individual privacy while enabling government agencies to analyze data. The panelists acknowledged that traditional methods for protecting privacy may be inadequate in today's world, and described technologies such as anonymization, encryption, identity management, immutable logs, and metadata that all help protect privacy while at the same time providing crucial tools for homeland security. The technologists cautioned, however, that technology is not a panacea, but rather just one way of helping to solve part of a problem. For example, under certain circumstances, in the absence of rules, processes, controls, oversight and audits, certain technology uses could raise privacy concerns.

The workshop concluded with a panel on how to build privacy protections into the government's use of commercial data. The panel was tasked with recommending a roadmap, and discussed building the roadmap on the fair information privacy principles of transparency, collection limitation, accountability, redress and due process rights. The panelists acknowledged the potential benefits for using commercial data, noting that DHS should define its legitimate purpose for using it. They urged DHS to build in privacy protections at the inception of programs using commercial data and to take measures to ensure that the policies governing the data use are implemented. Warning against mission creep, panelists suggested that there be rules in place to ensure that commercial data is used only for its originally intended purpose, and for which notice has been given to the public.

A full transcript of the workshop is available at: www.dhs.gov/privacy.⌘

Privacy Office Events

February 16-24, 2006

Asian-Pacific Economic Cooperation Symposium on Information Privacy in E-Government and E-Commerce, Hanoi, Vietnam

February 21, 2006

The European Privacy Officers Forum, Brussels, Belgium

March 7, 2006

Data Privacy and Integrity Advisory Committee Meeting, Washington, D.C.

March 14-16, 2006

US-Canada Binational Followup (Second) Meeting, Ottawa, Canada

March 27-28, 2006

Global Border Control Technology Summit 2, London, England

April 5, 2006

Department of Homeland Security Privacy Office Privacy and FOIA Workshop: Transparency and Accountability of Government Privacy Structures

Privacy & FOIA Workshop

Following the success of last fall's workshop on the use of commercial data for homeland security, the DHS Privacy Office will continue its privacy dialogues to inform DHS programs. This spring the Privacy Office will host its second workshop. The event will explore comparative government frameworks on transparency and accountability.

In conjunction with the 40th anniversary of the U.S. Freedom of Information Act (FOIA), the workshop will include a discussion of effective Privacy Notices and feature panels on FOIA and government accountability, international freedom of information laws, and transparency. The programs will include experts from U.S. and European public, private, and non-governmental organizations. The workshop is scheduled for the week of April 3rd. For more information, visit: **www.dhs.gov/privacy**.⌘

US/EU Joint Review Continued

Continued from front page

set of questions and answers concerning the privacy protections of the data. The discussions were candid and constructive.

There were several key findings in the Privacy Office's PNR report. First, CBP achieved full compliance with the representations in the Undertakings. Second, in cases where implementation took longer than anticipated, CBP has performed remediation at the request of the Privacy Office. Third, CBP has put in place an extensive privacy program that includes employee training and procedural and technical controls. Fourth, the Privacy Office has had no reports of any deliberate misuse of PNR information.

In the months following the Joint Review, the Privacy Office received positive feedback from many of our EU counterparts who expressed satisfaction with the thoroughness of the Joint Review.

In late January, the European Commission forwarded its final report on the Joint Review to the EU Parliment.

A copy of the Privacy Office's report, the U.S./EU Joint Statement, and the Undertakings are available on the Privacy Office's website at: www.dhs.gov/dhspublic/interapp/editorial/ditorial_0724.xml⌘

Meet the New Privacy Office Staff

Kenneth Mortensen

Privacy Expertise Grows with Addition of Senior Advisor

Kenneth P. Mortensen joined the Privacy Office as a Senior Advisor for privacy policy concerning a comprehensive framework for ensuring the effectiveness of information security and data privacy controls over technologies used by DHS. Additionally, he advises on data sharing initiatives for homeland security and the development of protocols for responsible information sharing and information management policies.

Before joining DHS, Mortensen practiced information privacy/data security law as a founding and managing partner of the law firm, Harvey & Mortensen. Additionally, he served as outside counsel for the Pennsylvania Office of Attorney General regarding technology and Internet matters.

Prior to forming his law firm, Mortensen taught information law at Villanova University School of Law as well as serving as Director of the Center for Information Law and Policy at Villanova.

Mortensen is coauthor of "Civil Litigation: Security" in the book *Data Security and Privacy Law: Combating Cyberthreats*, discussing legal issues arising from security breaches and cyber incidents.

Furthermore, Mr. Mortensen has served as a technology consultant for his own business and a hardware design engineer for Unisys Corporation, starting with Burroughs Corporation's large systems division. He earned his BSE in electrical and computer engineering from Drexel University and his joint JD/MBA from Villanova University. He is adjunct faculty at both Villanova University School of Law and West Chester University and he is a member of the Pennsylvania and New Jersey bars.⌘

Catherine Papoi

Privacy Office Welcomes Deputy Director for Disclosure and the Freedom of Information Act (FOIA)

Catherine M. Papoi has joined the Privacy Office as the Deputy Director of Departmental Disclosure and the FOIA. She is responsible for assisting the Director of Departmental Disclosure in program administration. Before joining the Privacy Office, she was a FOIA Specialist with the National Institute of Health (NIH), where she worked on agency FOIA matters since 2003.

At NIH, Papoi was responsible for drafting and issuing agency FOIA denials to requests for information, responding to the Department of Health and Human Services Appeal Authority on NIH FOIA appeals, and supervising and assisting the FOIA coordinators of NIH's 27 components to ensure consistent application of the statute and departmental regulations.

Prior to embarking on her career with the Federal government, she devoted three years to the Michigan Public Health Institute, working on a grant-funded project analyzing and cataloging all available tobacco litigation documents into a single large database. In addition, Papoi worked in the litigation practice group for the Michigan law firm Varnum, Riddering, Schmidt & Howlett, LLP, while completing her law degree at Michigan State University College of Law.⌘

Erica Perel

Attorney-Advisor Joins the Privacy Office

Erica Perel has joined the DHS Privacy Office as an Attorney-Advisor. She will provide legal advice and guidance on matters involving compliance with privacy and information disclosure laws and regulations.

Perel brings to the Privacy Office a breadth of public service experience, including ten years as a prosecuting attorney with the Kings County District Attorney's Office in Brooklyn, New York; service in the Giuliani Administration in New York City as an Associate Commissioner; and three years as Vice President of The Doe Fund, a nationally recognized non-profit that works with able-bodied, disenfranchised homeless persons.

Most recently, Perel served as a Policy Advisor at the Treasury Department's Office of Terrorism and Financial Intelligence, representing the department on anti-money laundering, counter-terrorist financing and policy issues. Perel staffed the President's Board on Safeguarding Americans' Civil Liberties, working with other agencies, including the DHS Privacy Office, on information sharing and privacy issues in light of the 9/11 Commission's recommendations.

Perel graduated from the University of Massachusetts and the American University, Washington College of Law.⌘

Billy Spears

Privacy Office Adds Director of Privacy Education & Training

Billy Spears serves as the Director of Privacy Education and Training. In this capacity, Spears is responsible for the design, execution, and overall coordination of detailed education and information outreach programs to achieve short- and long-range education and training objectives for the department. He works with each of the departmental components to identify privacy and FOIA training needs based on job functionalities and new and existing policies for all employees and contractors. In addition, he also works with the 22 components across the department to review and update existing privacy training programs. Spears is developing, and will manage, in-person training, video and web-based training, and a comprehensive program for identifiying employees that have gone through training and those that need to update their training.

Spears began his public service career in 1995. Before joining the Privacy Office, he served for eight years in the United States Marine Corps and later worked as the Disclosure Officer at the Federal Law Enforcement Training Center. Spears received his Bachelor of Science degree in Information Technology from National University in Phoenix, Arizona and his MBA from the University of Phoenix. ⌘

Privacy Office Training Moves Forward

Electronic Privacy Awareness Training Highlights Privacy Office Educational Program

The DHS Privacy Office continues to update and improve its educational programs on privacy and the Freedom of Information Act (FOIA) for the department. Currently, the Privacy Office has a number of training initiatives underway to align privacy and FOIA teaching with organizational priorities through the use of new training methodologies, including electronic and web-based learning. The new training methods will be added to existing routines through an incremental implementation process over the next few years.

Additionally, to improve the recognition of the privacy concerns that may occur within the course of DHS employees' daily duties, the Privacy Office is enhancing its outreach program to more fully address privacy awareness. The program will use information bulletins, awareness paraphernalia, and targeted privacy-oriented lectures to increase privacy consciousness across the department.

In connection with new training methods, a new electronic learning course entitled "Privacy Awareness" is under development. This course will be a twenty-five to thirty-five minute program reinforcing current privacy training for DHS employees and contractors on privacy awareness fundamentals. Additionally, the course gives a basic understanding of the privacy framework at DHS, each individual's responsibility, and the consequences for non-compliance with privacy policies. The use of scenarios in the course strengthens the understanding of the privacy objectives taught.

Once this initial course is developed, the Privacy Office will begin designing two additional electronic learning courses entitled "Privacy Act 101" and "Privacy Act 201". The first course will amplify general employee knowledge of the Privacy Act. The follow-up course, will educate supervisors about advanced business situations incorporating Privacy Act requirements. Furthermore, to supplement offline educational materials, the Privacy Office anticipates developing supplementary electronic learning courses regarding Privacy Impact Assessments, FOIA, and System of Records Notices.

All electronic learning courses will tie into the DHS Learning Management System (LMS), which supports the Presidential Management Agenda e-Learning Initiative and the DHS Learning and Development Strategic Plan for fiscal years 2006 through 2010.

This approach to achieving an enterprise-wide DHS LMS has three stages. The first stage implements a DHS Headquarters LMS. The second stage integrates DHS Organizational Elements (OE) without an LMS. The third stage migrates DHS OEs with legacy LMSs to the DHS LMS. This "gated" approach permits progression from one stage to the next building on the success of the previous stage and focusing on the functional requirements of each component of the department. The goal is to achieve a LMS with superior functionality and continuity, but running at a reduced cost than existing LMSs.⌘

International Audience Finding Common Ground With U.S. on Privacy

Partners Receptive to U.S. DHS Privacy Efforts

The Privacy Office continued its outreach to improve cooperation on privacy issues with our European and other international partners. In September, Chief Privacy Officer Nuala O'Connor Kelly; Maureen Cooney, Chief of Staff and Senior Advisor for International Privacy; and Director of International Privacy Programs John Kropf, led the U.S. delegation to the 27th International Conference of Data Protection and Privacy Commissioners in Montreux, Switzerland. Representatives from forty countries from around the world attended the conference. The U.S. attended for its third year, and the DHS Privacy Office was granted "observer" status for a second consecutive year. Kelly delivered a presentation on building privacy protections into counter-terrorism structures. She emphasized transparency and accountability as keys to maintaining privacy in such systems.

In October, Kropf traveled to Paris to represent DHS at the bi-annual meeting of the Organization for Economic Cooperation and Development Working Party on Information and Privacy. Here, the U.S. delegation reported on the status of the Enhanced International Travel Security System, a real-time information sharing system for travel documents.

In November, Acting Chief Privacy Officer Cooney and Kropf traveled to the EU to attend a series of meetings with data protection officials and others in Spain, Germany, and Brussels.

Highlights of the trip include a meeting with the Spanish Data Protection Administrator (DPA) and Vice-Chairman of the Article 29 Working Group, Louis Pinar and Mercedes Ortuno, Director of International Privacy. Cooney provided a summary of the Privacy Office's activities and priorities for the coming months. In Germany, members of the German Bundestag hosted the DHS team, which provided an overview of the U.S. privacy framework and the DHS Privacy Office. In Berlin, Cooney and Kropf met with the German DPA and Chairman of the Article 29 Working Group, Peter Schaar; DPA Deputy Hans Tischler; and Berlin DPA Alexander Dix, delivering a message of shared privacy principals between the U.S. and EU, despite different structures. Cooney also explained the Privacy Office's role as an ombudsman, working to counsel agencies on privacy matters and acting as an honest broker when handling questions or complaints from outside of DHS. Cooney ended the visit to Germany with an interview with "*c't Magazin f. Computertechnik*", a German technology magazine, and an address before a crowd of 50 participants from the German American Lawyers Association.

in Brussels, meetings were held with Peter Hustinx, European Data Supervisor of EU Institutions; Francisco Fonseca Morrillo, leader of the EU PNR Joint Review team; and Marjeta Jager, Director of Security, DG Transport and Energy, who also participated in the PNR review meetings in Washington, DC.⌘

Privacy Advisory Committee Issues First Reports

Reports on Commercial Data Usage, Secure Flight Highlight Recent Committee Meetings

The DHS Privacy and Integrity Advisory Committee has begun producing tangible results. Barely six months old at the time, the Committee adopted for release its first report, concerning the use of commercial data to reduce false positives in screening programs, at its September meeting in Bellingham, Washington. At the following meeting in Washington, DC, in December, the Committee issued its second report in three months, this one concerning the Secure Flight program.

Commercial Data Report Adopted

A false positive is the misidentification of an individual as someone who is on a terrorist watchlist, when that individual is not. The report examined whether the department's use of commercial data could reduce false positives and, therefore, increase the effectiveness its passenger screening programs.

The report presented the benefits and risks associated with commercial data use and discussed issues that DHS should examine when considering the use of commercial data. The committee presented several recommendations to govern the use of commercial data, including: minimization, strict access control, transparency, and applying Privacy Act restrictions.

Highlights of the Bellingham, WA Meeting

Trevor Shaw, Director General of the Audit and Review Branch of the Office of the Privacy Commissioner of Canada, presented an international perspective on privacy and homeland security. According to Shaw, the Canadian perspective on privacy views ensuring security and guarding fundamental values, such as privacy, as essential duties of government. Later, he expressed his belief that Canada and the United States share the same interest in sustaining privacy and protecting democratic values.

Justin Oberman, Assistant Administrator at the DHS Transportation and Security Administration (TSA) gave an update on the Secure Flight program. He noted that TSA was in the process of amending the privacy documents for Secure Flight prior to live testing the program. Oberman then reiterated the key privacy principles for Secure Flight: focusing only on known or suspected terrorist threats, collecting only necessary information, and keeping personal information only as long as necessary.

The meeting included two panels, one on the use of Radio Frequency Identification (RFID) technology by DHS, and the other on Risk-Based Analysis and Communication. Guests on the RFID panel included Michael Westray from the US-Visit program at DHS, Deirdre Mulligan from the University of California-Berkley Law School, Lee Tien from the Electronic Frontier Foundation, and Peter Neumann from SRI Computer Science Laboratory. The panel discussed the privacy concerns associated with using RFID technology to track entry into, and exit from, the U.S. The Risk-Based Analysis panel included John Mueller from The Ohio State University, Paul Slovic from Decision Research and Detlof von Winterfeldt from the University of Southern California, who discussed the issues associated with defining, communicating, and asessing risk, as well as the privacy impacts of risk, vulnerability, and consequence analyses.

Secure Flight Report Adopted

At the December meeting, the Committee adopted its report "Recommendations on Secure Flight." The report contained five recommendations: transparency, a narrowly defined mission, data minimization, proactive redress, and holistic management.

Highlights of the Washington, DC Meeting

Paul Rosenzweig, Counselor to the DHS Assistant Secretary for Policy addressed the committee on behalf of Secretary Michael Chertoff. Rosenzweig told the Committee that DHS desires security consistent with American freedoms and values, including privacy. Speaking on the use of technology and data analysis, he said both may raise privacy concerns, but are necessary for homeland security.

> *"As we engage technology to extend our reach, we also need to expand our appreciation and protection of privacy."*

Delivering the Secretary's prepared remarks, Rosenzweig said, "As we engage technology to extend our reach, we also need to expand our appreciation and protection of privacy."

The meeting also featured two panels, one on data analytics, and the other on redress at DHS. Guests on the data analytics panel included Xuhui Shao of ID Analytics, Jeff Jonas of IBM, Mary DeRosa from the Center for Strategic and International Studies, and Nancy Libin of the Center for Democracy and Technology. The redress panel included Virginia Skroski from TSA's Redress Office, Caroline Hunter from the Citizen and Immigration Services Ombudsman Office, Sandra Bell of Customs and Border Protection's Office of Regulations and Rulings, and Jennifer Barrett of Acxiom. The data analytics panel discussed a definition of data analytics, the importance of direct reason data sharing, data anonymization, the importance of immutable audit logs, the limited role of predicate-based data mining in homeland security, and policy issues associated with data mining. The redress panel discussed the redress processes in place at DHS and responded to the Committee's questions regarding how affected individuals go through these processes, improving redress, and consistency in redress processes.

The meeting concluded with a panel on cross-border cooperation featuring German Federal Data Protection Commissioner Peter Shaar and Spanish Data Protection Authority representative Augustin Puente. In his remarks, Shaar discussed the three pillars of European privacy and touched on concerns regarding the U.S. privacy framework. Shaar noted that the U.S. and EU share the same privacy principles. Puente followed, stressing the similarities between the U.S. and the EU. He noted that both the U.S and most European countries are part of OECD, and thus share those privacy principles. Puente posited that cross-border

See PRIVACY ADVISORY COMMITTEE, page 6

Privacy Office Staff

Maureen Cooney
Acting Chief Privacy Officer &
Chief FOIA Officer

Sandra L. Hawkins
Administrative Officer

Elizabeth Withnell
Chief Counsel to the Privacy Office

Toby Milgrom Levin
Senior Advisor

Kenneth P. Mortensen
Senior Advisor

Tony Kendrick
Director, Departmental Disclosure & FOIA

John Kropf
Director, International Privacy Programs

Peter Sand
Director, Privacy Technology

Rebecca Richards
Director, Privacy Compliance

Billy Spears
Director, Privacy Education & Training

Catherine Papoi
Deputy Director, Departmental
Disclosure & FOIA

Erica Perel
Attorney-Advisor

Lane Raffray
Privacy Policy Analyst

Anna Slomovic
Senior Privacy Strategist

John Sanet
Senior Privacy Advisor

Nathan Coleman
Privacy Analyst

Kathleen Kavanaugh
Privacy Researcher

Tamara Baker
Event Executive

Sandra Debnam
Administrative Assistant

Erin Odom
Administrative Assistant

Vania Lockett
Senior FOIA Specialist

Sarah Mehlhaff
FOIA Specialist

Rasheena Spears
FOIA Specialist

Stepahnie Kuehn
FOIA Specialist

Mark Dorgran
FOIA Specialist

Shannon Snypp
FOIA Specialist

Component Privacy Officers

Lisa Dean
Privacy Officer, TSA

Elizabeth Gaffin
Privacy Officer, CIS

Andy Purdy
Privacy Officer, NCSD

Steve Yonkers
Privacy Officer, US-VISIT

Website: http://www.dhs.gov/privacy/
Email: privacy@dhs.gov
Telephone: 571-227-3813
Facsimile: 571-227-4171

Privacy Office Takes Lead On Biometrics

Privacy Office Involved Internally, Externally, Internationally

Even before September 11th brought an increased national and international focus on identity and security, biometrics were already part of the debate. The public increasingly expects that information technology will provide transparent recognition and secure identities, replacing physical identities with digital ones. Because of its inherent connection to the individual, the use of biometrics raises privacy concerns. The Privacy Office serves to manage and minimize these risks to privacy while promoting the technology's usefulness.

The Privacy Office focuses its review of DHS use of biometric technologies at both micro and macro levels. At the micro level, the Privacy Office reviews every system proposal within DHS. At the macro level, the Privacy Office coordinates privacy policy and awareness regarding biometric technology. As such, the Privacy Office participates in the DHS Biometrics Coordination Group (BCG), which coordinates the use of biometric technology across the Department, and works with this group and each participant to ensure system functionality maps closely to privacy protections.

External to the Department, the Privacy Office leads a multi-agency discussion of privacy and biometrics through the National Science and Technology Council's Biometrics Subcommittee. Here, the Privacy Office is developing a paper that communicates how to integrate privacy protections and biometric technology.

The Privacy Office is very much involved internationally as well. In October, Acting Chief Privacy Officer Maureen Cooney spoke before the RSA Conference in Vienna, Austria, discussing privacy within the context of biometrics. Because biometric identifiers are characteristics of the human body, they are the most elemental of identification keys. As such, if biometrics are to be used, Cooney said,"there is no doubt that privacy must be central to the development of biometrics."

She expressed confidence that with a privacy-centric approach, with the appropriate controls in place throughout the system development cycle, biometrics could enhance privacy.

"Because of the strong link between the biometric information and an individual, identity theft could become more difficult to perpetuate," Cooney said.

Cooney cited DHS's US-VISIT as a program sucessfully utilizing biometrics while safeguarding privacy, noting that US-VISIT has currently processed over 34 million travelers and has received approximately 75 redress requests.

In December, at the invitation of the European Commission, John Kropf, Director of International Privacy Programs, and Senior Advisor Ken Mortensen represented DHS in a biometrics and privacy workshop in Brussels, Belgium. The workshop featured over 70 participants from Europe, Japan and the United States, and included presentations on technical, legal, social and philosophical aspects of biometrics. The presentations stressed building privacy into the development of biometric technology to facilitate compliance with fair information principles.⌘

Privacy Advisory Committee Continued

data sharing could be improved through increasing cooperation among countries and focusing on practical solutions, balancing privacy protection principles, and the purposes for which data is used.

The next Data Privacy and Integrity Advisory Committee meeting is scheduled for March 7, 2006, in Washington, DC. For more information about the Committee, visit www.dhs.gov/privacy.⌘

Talk to us!

Need help writing PIAs? Have a question about privacy? Or would you like to have the DHS Privacy Office make a presentation to your organization, please contact us at 571-227-3813. Or feel free to contact us via email at privacy@dhs.gov.

If you would like to make a presentation to the Privacy Officers and Freedom of Information Act Officers for the Department of Homeland Security, please contact the DHS Privacy Office at 571-227-3813 or privacy@dhs.gov. Please note that topics should be related to privacy or FOIA issues rather than privacy or FOIA products or services.