Setting the Record Straight:
U.S. Department of Homeland Security Policies on Protecting Privacy

Lauren Saadat and Shannon Ballard[1]

As published in the November 2007 issue of *Data Protection Law & Policy*

A. Reality v. Misconception

The privacy policies of the U.S. Department of Homeland Security (DHS) have long been a focus of misplaced criticism in the European press and from European Data Protection Authorities. This is ironic, because DHS has been a privacy leader in the U.S. Government and embodies policies that arguably protect privacy to a greater degree than those of similar European agencies. It may be that the very transparency of DHS practices has drawn disapproval that is not forthcoming to less transparent agencies overseas. Contrary to the way the issue has been framed by its critics, DHS has no policy that singles out EU citizens over other non-U.S. persons. Nonetheless, this article is written to address concerns the European public may have about DHS privacy policies.

DHS privacy policy is implemented through the Privacy Office, which was the first statutorily mandated Privacy Office at any U.S. Federal agency. Its mission is to minimize the impact on the individual's privacy, particularly the individual's personal information and dignity, while serving the DHS mission to secure America. More specifically, statutory duties include: 1) assure that new technologies do not erode privacy; 2) assure that personal information in Privacy Act Systems of Records is handled in compliance with the Fair Information Principles as set out in the Privacy Act;[2]

---

[1] Lauren Saadat and Shannon Ballard are Associate Directors for International Privacy Policy at the U.S. Department of Homeland Security.

[2] The FIP were first articulated in the 1973 report by the U.S. Department of Health, Education, and Welfare advisory committee. The report listed the following practices:

- Collection limitation principle--data should be obtained lawfully and fairly;
- Data quality principle--data should be relevant to the purposes for which it will be used, accurate, complete and up-to-date;
- Purpose specification principle--the purposes for which data will be used should be identified at the time of collection;
- Use limitation principle--personal data should not be used for purposes other than those specified except with the consent of the individual or by authority of law;
- Security safeguards principle--procedures to guard against loss, corruption, destruction or misuse of data should be established;
- Openness principle--it should be possible to acquire information about the collection, storage and use of personal data;
- Individual participation principle--the data subject normally has a right of access and to challenge data relating to her; and
- Accountability principle--a data controller should be designated and accountable for complying with measures to give effect to the principles.

The FIPs served as the basis for the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the Committee of Ministers of the Organization for Economic Cooperation and Development (OECD Guidelines). The OECD Guidelines are the basis for the EU's 1995 Data Protection Directive.

3) evaluate new legislation on personal information; 4) report to Congress; and 5) coordinate with the DHS Civil Rights and Civil Liberties Office.

B. Foundation of Transparency

Transparency is the foundation for DHS privacy practices. Perhaps no other agency provides as much notice to the world as DHS does on its privacy systems. All of its systems, whether the Automated Targeting System that contains Passenger Name Records, or any other system that collects personally identifiable information, are subject to the oversight of the Chief Privacy Officer and the requirements of U.S. privacy laws.

1. Privacy Act: Transparency at the Front End

The Privacy Act of 1974 provides substantial notice, access, and redress rights for citizens and legal residents of the U.S. (herein U.S. persons) whose information is held by a branch of the federal government. DHS made a groundbreaking policy commitment to extend Privacy Act protections to non-U.S. persons, which is posted on its website.[3] Of particular interest to European citizens may be the requirement to publish notice of all systems of records (SORNs) in the Federal Register for public comment. A SORN is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each SORN that the agency maintains, and the routine uses that are contained in each system to make agency recordkeeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist the individual to more easily find such files within the agency. Any person, regardless of citizenship, may submit public comments to proposed SORNs. Any person who is interested in what systems of records are kept by DHS may access the SORNs on the DHS website.[4]

2. E-Government Act: Transparency in Detail

The E-Government Act of 2002 recognized that technological advances in computers, networks, and the Internet have important ramifications for the protection of personal information contained in government records and systems. The Act mandates an assessment of the privacy impact of any substantially revised or new Information Technology System. The document that results from these mandated assessments is called a Privacy Impact Assessment (PIA).

The PIA is one of the most important instruments through which DHS establishes public trust in its operations. Through the PIA, the DHS Chief Privacy Officer ensures that technologies developed and used by DHS sustain and do not erode privacy protections. Specifically, the PIA serves three functions in the DHS context. First, it is used for transparency so that the public can learn about what DHS is doing with personally identifiable information. DHS PIAs are drafted to be clear, concise, and understandable by nonprofessionals. DHS has published all but a few national security system PIAs on its web site.

---

[3] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

[4] http://www.dhs.gov/xinfoshare/publications/gc_1185458955781.shtm

Second, the PIA is used to assess the privacy impact of DHS programs at their inception. Through the PIA, DHS Privacy Compliance Officers have a structured conversation about what information the program is going to collect, about whom, and for what purposes. This process begins early in the development of the program and continues through until the program is ready to become operational. Using the PIA, the DHS Privacy Office assesses the impact and provides recommendations or requirements for mitigating privacy risks. All PIAs must be reviewed an approved by the Chief Privacy Officer before the program is allowed to go operational.

The third function of the PIA is to show ongoing compliance with the privacy requirements placed on DHS by Congress, the Office of Management and Budget (OMB), and the public at large. Programs comply with the PIA requirements not just because it is the right thing to do, but because there are budgetary consequences to not complying. As part of the annual budget process, the Privacy Office reviews DHS programs for compliance. Some programs have been put on hold until their PIAs are completed and submitted to Congress or OMB. In fact, a number of programs have been canceled or suspended because they didn't follow the privacy compliance process.

DHS has developed Official Guidance to use in drafting PIAs, with the current version effective May 2007.[5] Since its inception, the Privacy Office has approved 108 PIAs, all but two (for national security reasons) are published on the DHS website.[6] Citizens of any country may access these PIAs.

3. Freedom of Information Act: Transparency at the Back End

The Freedom of Information Act (FOIA) upholds the principle that persons have a profound and fundamental right to know what the government is doing. Any person, regardless of citizenship or place of residence, has the right to query a federal agency about documents and records. DHS takes this responsibility very seriously; in the period of October 1, 2005 – September 30, 2006, DHS spent over $28 million processing 111,943 requests. DHS publishes Annual FOIA Reports, available at its website.[7] EU citizens that wish to know what records DHS may hold about them should access the guidance for making FOIA requests on the DHS website.[8]

4. Redress for All: Traveler Redress Inquiry Program (TRIP)

An essential component of DHS accountability is the TRIP program, through which inaccuracies may be brought to the attention of the record keepers. Most EU citizens will provide their information to DHS in the course of travel to or from the U.S. TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like

---

[5] http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm

[6] While PIA's involving national security systems are exempt from PIAs, DHS made a policy commitment that programs must be reviewed and approved by the CPO. This constitutes an extremely small number of DHS's overall PIAs.

[7] http://www.dhs.gov/xinfoshare/publications/editorial_0514.shtm

[8] http://www.dhs.gov/xfoia/editorial_0579.shtm

airports and train stations – or crossing U.S. borders, including denied or delayed airline boarding, denied or delayed entry into and exit from the U.S. at a port of entry or border checkpoint, or continuous referral to additional (secondary) screening. TRIP is also a central gateway to address watch list misidentification issues. Travelers may access TRIP at http://www.dhs.gov/trip. The information a traveler provides is of course, shared in accordance with the provisions of the Privacy Act, and as established in the PIA published for DHS TRIP.[9]

C. A Few Words about Passenger Name Records (PNR)

The U.S.-EU PNR agreement, and the use of PNR data in the Automated Targeting System (ATS) program, has perhaps generated more negative press in Europe than any other DHS program. DHS receives PNR on all passengers on all international flights, regardless of nationality. PNR consists of information that passengers provide to airlines for travel reservations, either directly or via a travel agent. The PNR agreement and the ATS SORN and PIA are available to the public on the DHS website, so anyone may know what information is gathered and how it is used. Through the FOIA process described above, concerned travelers may find out what PNR data DHS holds, and through the TRIP program, they may request to have any inaccuracies corrected.

Many critics have accused DHS of routinely collecting sensitive information, such as race, religion, sexual orientation, meal preference, and political or union affiliation, through PNR. This is simply not the case. The public can easily confirm this, through reading the PNR agreement, letter of explanation,[10] the ATS SORN and PIA, or by availing themselves of FOIA. In any case, such information would only exist if the traveler provided it in making the reservation. Even then, if an individual provided it, DHS routinely filters it out. The only condition under which DHS may access an individual's sensitive PNR information, should it exist, is if that individual is the subject of a terrorism or criminal investigation. Of course, in such exceptional circumstances, DHS and other law enforcement authorities will seek information far beyond the suspect's PNR.

D. CONCLUSION: Privacy AND Security

DHS representatives are often asked whether it is true that whatever is done to strengthen security must be at the expense of privacy – as if it were a zero sum game. DHS policy is to uphold both privacy and security, because both are fundamental rights and one positively impacts the other. Our border control officers must screen some 80 million travelers who fly to the U.S. annually. As required by law, DHS collects only information that is relevant and necessary about each visitor – just enough to help decide who might be a potential security risk. When compared to the alternatives (i.e., searching everyone, searching no one, or the hit-or-miss strategy of random searches) this is clearly the best way to maximize security while at the same time maximizing privacy.

A large part of our mission necessarily involves relating to and working with partners all over the world. In testimony before the EU Parliament last May, Secretary Chertoff said

[9] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf
[10] http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usltrtoeu.pdf

"None of us want to forsake our civil liberties in the name of security. On the contrary we seek security that is strong and effective, but consistent with the freedoms and values we all cherish as free and democratic nations." An unbiased examination of DHS privacy policies, as compared with similar agencies in other countries, must note that perhaps no other agency provides as much transparency and access. Next time there is a question about how DHS handles personally identifiable information, remember it is there in plain sight for all the world to see.