Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

January 7, 2009

PRIVACY POLICY GUIDANCE MEMORANDUM
Memorandum Number: 2007-1 (As amended from January 19, 2007)

MEMORANDUM FOR: DISTRIBUTION LIST

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons

I. PURPOSE

This memorandum sets forth the policy of the DHS Privacy Office regarding privacy protections afforded to non-U.S. persons for information collected, used, retained, and/or disseminated by the Department of Homeland Security in so-called "mixed systems."[1]

II. AUTHORITY

The Chief Privacy Officer has primary authority under Section 222 of the Homeland Security Act of 2002[2] for privacy policy at DHS. Section 222 gives the Chief Privacy Officer plenary authority to ensure that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information, and to ensure that personal information in Privacy Act systems is handled in full compliance with the fair information practices as set out in the Privacy Act. In addition, Section 222 requires the Chief Privacy Officer to conduct privacy impact assessments on proposed rules of the Department. The policy that the Chief Privacy Officer has developed for the treatment of information about all persons is consistent with and derives from this statutory authority.

---

1 This document represents the views of the DHS Privacy Office pursuant to its statutory mandate under Section 222 of the Homeland Security Act of 2002, as amended.

2 Homeland Security Act of 2002, P.L. 107-296, 116 Stat. 2155 (November 25, 2002) (enacted in general by Congress to create the Department of Homeland Security).

III. PRIVACY POLICY

As a matter of law, the Privacy Act of 1974 ("Privacy Act"), 5 U.S.C. § 552a, as amended, provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPRs). The Privacy Act does not cover visitors or aliens. As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.

Under this policy, DHS components will handle non-U.S. person PII held in mixed systems in accordance with the fair information practices, as set forth in the Privacy Act. Non-U.S. persons have the right of access to their PII and the right to amend their records, absent an exemption under the Privacy Act; however, this policy does not extend or create a right of judicial review for non-U.S. persons.

DHS components shall develop mixed systems in conformity with the fair information practices embodied in the Privacy Act, keeping in mind the Act's exemptions for law enforcement systems or in cases of any national security need as determined by the Secretary, and shall be analyzed pursuant to the requirements of Section 208 of the E-Government Act to ensure that privacy protections are built into the systems. This policy shall be applied consistent with the Privacy Act's exemption of intelligence files and data systems devoted solely to foreign nationals or maintained for the purpose of intelligence activities made subject to the provisions and protections of Executive Order 12333.

For the purposes of this policy the following terms shall have the following meanings:

- "DHS Information Systems" shall mean an Information System operated, controlled, or directed by the U.S. Department of Homeland Security. This definition shall include information systems that other entities, including private sector organizations, operate on behalf of or for the benefit of the Department of Homeland Security;
- "E-Government Act" shall mean Public Law, P.L. 107-347, 116 Stat. 2899, as enrolled on December 17, 2002, and any amendments;
- "Identifiable Form" shall have the same meaning as under Section 208 of the E-Government Act of 2002, as amended;
- "Information System" shall have the same meaning as defined under 44 U.S.C. § 3502(8), as amended.
- "Mixed System" or "Mixed Systems" shall mean any System of Records that collects, maintains, or disseminates information, which is in an identifiable form, and which contains information about U.S. Persons and non-U.S. Persons.
- "Non-U.S. Person" shall mean any individual that is not a United States Citizen or LPR;

- "Privacy Act" shall mean 5 U.S.C. § 552a, as amended. "System of Records" shall have the same meaning as found in the Privacy Act, 5 U.S.C. § 552a(a)(5). "The term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

IV. ESSENTIAL BACKGROUND

Under the Privacy Act, a federal agency must provide certain protections to personally identifiable information that is collected, maintained, and used by a Federal agency. The language of the Privacy Act states that "[n]o agency shall disclose any record which is contained in a 'System of Records' by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains…." A "system of records" is defined by the Act as a collection of records about an "individual from which information is retrieved by name or personal identifier," and, importantly, an "individual," is defined by the Act to be a citizen of the United States or a Legal Permanent Resident.[3]

A. Consistent with OMB Guidance

Shortly after the enactment of the Privacy Act, the Office of Management and Budget (OMB), the entity responsible for overseeing implementation of the Act, issued a comprehensive set of guidelines to the heads of all Executive Departments on their responsibilities under the Act. In cases where agencies maintain mixed system of records -- that is a system of records with information about both U.S. persons and non-U.S. persons -- OMB encouraged Federal agencies to treat the entire system as covered under the Privacy Act. In its 1975 guidance, OMB provided: "Where a system of records covers both [U.S. persons] and [non-U.S. persons], only that portion, which relates to [U.S. persons] is subject to the Act, but agencies are encouraged to treat such systems as if they were, in their entirety, subject to the Act."[4]

An agency treats mixed systems as Privacy Act systems, in part, because of inherent difficulties in determining an individual's current citizenship status, which may change over time through naturalization or adjustment. While an agency may apply the Privacy Act to a mixed system, such a policy decision does not and cannot extend all Privacy Act rights to non-U.S. persons. Thus, while all individuals would benefit from the transparency that accompanies notice of an agency's system of records as well as the access and correction opportunities, a non-U.S. person does not have legal standing to seek a judicial remedy, based on the statutory definition of "individual" for Privacy Act

---

[3] 5 U.S.C. § 552a(a)(2), which provides:
"(2) the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence;"

[4] Circular A-108, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28951 (July 9, 1975).

purposes. Nevertheless, by publishing system notices that apply to mixed systems and provide means of access and correction, agencies demonstrate tangible implementation of the fair information practices that are reflected in the Privacy Act and that also form the basis of international privacy frameworks promoted by the U.S. (*e.g.*, the 1980 OECD Guidelines on the Protection of Transborder Information Flows of Personal Data and the 2003 APEC Privacy Framework).

B. Consistent with DHS and Other Agency Practice

Many legacy agencies of DHS have maintained mixed systems and, pursuant to their discretion under OMB guidance, have treated the systems as covered by the Privacy Act. By treating these systems as Privacy Act systems, component agencies have implemented efficient and uniform business practices concerning information handling, eliminating the need to maintain two parallel systems serving much the same purpose, for U.S. citizens and LPRs and all other individuals. The U.S. Citizenship and Immigration Services, one DHS component created from the former Immigration and Naturalization Service, is an example of a component that has published Privacy Act system notices covering mixed systems.

DHS is not unique in its application of Privacy Act coverage to mixed systems. Other agencies such as the Departments of Justice and State also apply the Act to mixed systems.[5]

V. POLICY IMPLICATIONS: ADVANCES DHS GOALS

A. Standardizing Existing Department Practice Supports Data Integrity

Department-wide adoption of this policy will standardize an existing practice and sub-agency policy that currently exists in DHS programs such as US-VISIT. Application of fair information practices to mixed systems supports the Department's interest in data integrity. For example, allowing for access and correction will reduce inaccuracies and, as an operational matter, false positives.

B. Advances Cross Border Information Sharing and Facilitates Travel and Trade

Early in DHS's existence, the Chief Privacy Officer committed to following OMB guidance on mixed systems. Major programs such as US-VISIT, for example, embedded Privacy Act coverage in its mixed system.[6] DHS was mindful that such a policy would not only build trust in the traveling public, but it would also advance our strategic goal of

---

[5] Examples for the Department of Justice include the following systems: Executive Office of Immigration Review Records (EOIR) Records, INTERPOL (USNCB) Records, and International Prisoner Transfer Case Files/International Prisoner Transfer Tracking Records. Examples for the Department of State include Visa Records and Refugee Case Records.

[6] As of January 2006, the US-VISIT system contains records on 51 million individuals who at the time of their enrollment were not U.S. persons.

cross-border information sharing. Since the Department intended to rely heavily on access to foreign visitor information, this policy assured foreign partners that their citizens' information would be safeguarded, which would make information sharing more likely. As with the U.S. system, our allies and friends have their own obligations to ensure the privacy of their citizens' information. Failure to offer DHS's partners such commitments could have adverse implications for long-term Department objectives.

C. Protection of U.S. Persons' Privacy Overseas

Formalizing the Department's mixed use privacy policy will have direct benefits for DHS's obligation to protect information on U.S. persons traveling abroad. Reciprocity is a fundamental condition of international relations and one the U.S. Government has followed with the treatment of persons and exchanges of information. Indeed, it is a fundamental structure of many international agreements[7] including arms control, trade and commerce, and law enforcement. Even the Supreme Court has observed, "Public officials should bear in mind that 'international law is founded upon mutuality and reciprocity. . . .'"[8]

Reciprocity is relevant here because various foreign partners are expected to request personally identifiable information on U.S. persons entering their countries. Indeed, the United Kingdom and France are in the preliminary stages of implementing their own programs for using Passenger Name Records data on travelers entering their countries. If DHS wants foreign partners to afford protections to data collected about U.S. citizens, a positive commitment to honor privacy protections for non-U.S. persons, as demonstrated through application of the Privacy Act to mixed systems, will improve the chances for success. In short, DHS wants to be in a position to be able to say "we'll give your people the same privacy you give our people." To do otherwise, would put the Department in an untenable position of seeking a double standard.

D. E-Government Act of 2002 Reinforcement

Separate from the Privacy Act and its coverage, Section 208 of the E-Government Act of 2002 ("E-Gov Act") requires that privacy impact assessments be conducted on all new Federal systems collecting information in identifiable form[9] and on any existing Federal systems that are making major changes, collecting new types of information, or changing system uses.[10] The E-Gov Act does not limit its coverage only to U.S. persons; instead, it focuses on information systems. Thus, the E-Gov Act requires that an information system be analyzed for privacy risks based on the architecture of the system itself and its associated collections and uses, without regard to whom the system covers. And the

---

7 Arthur Nussbaum, *A Concise History of the Law of Nations* (The Macmillion Co., New York, 1954); Robert O. Keohane, *Reciprocity in International Relations*, 40 INT'L ORG. 1 (1986).

8 *Breard v. Pruett*, 134 F.3d 615, 622 (4th Cir.), cert. denied sub nom. *Breard v. Greene*, 118 S.Ct. 1352 (1998) quoting *Hilton v. Guyot*, 159 U.S. 113, 130 (1895).

9 § 208(d) DEFINITION.—In this section, the term ''identifiable form'' means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. (44 U.S.C. § 3501, note)

10 *Id*., § 208(b)(1)(A).

OMB guidance on Section 208 of the E-Gov Act expressly recognizes that agencies may extend coverage to other than U.S. citizens.[11] The Privacy Office's policy and guidance for conducting a Privacy Impact Assessment ("PIA") on DHS systems is to review the privacy impact of all new or changing data systems and not to limit such reviews to those systems that solely collect information about U.S. persons. This policy regarding mixed systems is consistent with our policy on PIAs.

[11] Office of Management and Budget, M03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, at n.1 (Sept. 26, 2003).