DEPARTMENT OF HOMELAND SECURITY

Border and Transportation Security Doctorate

Docket No. BTS 03-01
Interim Final Rule and Notice

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on January 5, 2003, the Department of Homeland Security ("DHS") announced the implementation of the United States Visitor and Immigrant Status Technology ("US-VISIT").[1] Pursuant to the DHS notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge DHS to define how Privacy Act obligations affect the program, to consider the significance of international privacy standards in the collection and use of personal information by the agency on non-U.S. citizens, and to prohibit the expansion of US-VISIT uses outside the program's defined mission.

DHS Should Clarify How US-VISIT Will Affect Individuals Protected by the Privacy Act

The Privacy Act was intended to guard the privacy of lawful permanent residents and U.S. citizens against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a

[1] Interim Final Rule and Notice, 69 Fed. Reg. 467 (Jan. 5, 2004).

personal and fundamental right protected by the Constitution of the United States."[2] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[3]

US-VISIT inevitably will collect information on some number of foreign nationals who will eventually become lawful permanent residents and U.S. citizens. Information about those individuals maintained within US-VISIT eventually will become subject to Privacy Act protections. DHS must explain how it intends to maintain and use the information of individuals obtained from US-VISIT when those individuals later become protected by the Privacy Act.

DHS should also clarify how long it intends to retain information initially collected for US-VISIT use once an individual becomes a lawful permanent resident or U.S. citizen. EPIC urges DHS to consider expunging an individual's information from the US-VISIT program when that person becomes a lawful permanent resident or U.S. citizen. When an individual's information is no longer useful for US-VISIT purposes, there is no reason for DHS to maintain that information in the US-VISIT system. In fact, retaining such information may violate the Privacy Act requirements that an agency "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President[.]" 5 U.S.C. § 552a(e)(1). For this reason, EPIC recommends that DHS develop guidelines for deleting records of those who become lawful permanent residents or U.S. citizens from the US-VISIT system.

---

[2] Pub. L. No. 93-579 (1974).
[3] *Id*.

As it Implements US-VISIT, DHS Should Observe International Standards Governing the Collection and Use of Personal Information on Non-U.S. Citizens

While no U.S. law currently requires DHS to protect the privacy of non-U.S. citizens as the agency develops and deploys US-VISIT, EPIC urges DHS to consider the application of international privacy standards to the collection and use of personal information obtained for non-U.S. citizens. The international community has recognized time and time again that all individuals have rights in their personal information, regardless of nationality.

The Universal Declaration of Human Rights ("Universal Declaration") provides that no individual "shall be subjected to arbitrary interference with his privacy," and that "[e]veryone has the right to protection of the law against such interference or attacks."[4] Furthermore, "no distinction shall be made on the basis of the political, jurisdictional, or *international* status of the country or territory to which a person belongs"[5] (emphasis added). The United States was a key architect of the Universal Declaration and one of the original signatories. It is thus surprising to find our nation deploying a system that violates the Universal Declaration by encroaching upon the privacy of individuals based on their lack of U.S. citizenship, and failing to provide them rights in their personal information held by the United States.

Similarly, the OECD Privacy Guidelines of 1980 ("OECD Privacy Guidelines") apply to "personal data, whether in the public or private sectors, which, because of the

[4] United Nations, Universal Declaration of Human Rights, G.A. Res. 217A(III), U.N. GAOR, 3d Sess., U.N. Doc. A/810 (1948), art. 12, reprinted in M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2003 318 (EPIC 2003) [hereinafter PRIVACY LAW SOURCEBOOK].

[5] *Id*., art. 2 at 318.

manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties."[6] The OECD Privacy Guidelines require, among other things, that there should be limitations on the collection of information; collection should be relevant to the purpose for which it is collected; there should be a policy of openness about the information's existence, nature, collection, maintenance and use; and individuals should have rights to access, amend, complete, or erase information as appropriate.[7] US-VISIT, as currently designed, will deny non-U.S. citizens the fundamental protections of these internationally recognized standards.

The United Nations Guidelines for the Regulation of Computerized Personal Files of 1990 ("UN Privacy Guidelines") recognize many of the same rights in information as the OECD Privacy Guidelines provide, providing in addition that "data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, philosophical and other beliefs . . . should not be compiled."[8] The US-VISIT program may collect and use information of this nature to evaluate whether visitors may enter the United States, a use that would clearly violate the UN Privacy Guidelines.

In addition, the European Union Data Protection Directive ("EU Directive") recognizes a right to privacy in personal information and establishes protections for

---

[6] Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Trans-Border Flow of Personal Data, OECD Doc. 58 final (Sept. 23, 1980), art. 3(a), reprinted in PRIVACY LAW SOURCEBOOK at 330.

[7] *Id*., Basic Principles of National Application at 331.

[8] United Nations, G.A. Res. 45/95, Guidelines for the Regulation of Computerized Personal Files (Dec. 14, 1999) prin. 5, reprinted in PRIVACY LAW SOURCEBOOK at 368.

information collected from all individuals, regardless of nationality.[9] Like both sets of Guidelines, the EU Directive recognizes an individual's right to access information and requires that information be kept accurate and timely.[10] The EU Directive also requires that information be relevant to the purpose for which it is collected.[11] By neglecting to give non-U.S. citizens rights in information about them used in the US-VISIT program, the United States has failed to comply with this widely recognized legal regime for privacy protection.

The United States is a signatory of the Universal Declaration, OECD Privacy Guidelines, and UN Privacy. The United States's collection and use of personal information of non-U.S. citizens through the US-VISIT program violates these guidelines, as well as the EU Directive, and suggests a disregard for international privacy laws and human rights standards.

DHS Must Prohibit Mission Creep in the US-VISIT Program

The Interim Final Rule and Notice notes that DHS is "particularly interested in comments on . . . uses for the biometric information to be collected[.]"[12] EPIC urges DHS to confine its use of biometric data strictly to the purposes for which it is collected, and not to expand uses of US-VISIT data through "mission creep" -- the tendency of

[9] Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, reprinted in PRIVACY LAW SOURCEBOOK at 371.

[10] *Id*., art. 6 at 384.

[11] *Id*.

[12] 69 Fed. Reg. 476.

government agencies to expand the use of personal information beyond the purpose for which it was initially collected. DHS has already succumbed to mission creep in the development of another program, the Computer Assisted Passenger Prescreening System ("CAPPS II"). Deputy Secretary of DHS Admiral James Loy discussed the potential for CAPPS II mission creep in Congressional testimony, stating that "mission creep, if you will, is one of those absolute parameters that . . . I am enormously concerned about and we will build such concerns into the privacy strategy that we will have for CAPPS II."[13] Admiral James Loy, then Administrator of the Transportation Security Administration, assured Congress that CAPPS II was intended to be an aviation security tool, not a law enforcement tool.[14] Despite these assurances, just three months later the CAPPS II system included a carve-out for a purpose beyond its defined mission. A Privacy Act Notice published by the Transportation Security Administration on August 1, 2003 stated that "[a]fter the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence many also be analyzed in the context of this system."[15] On January 27, 2004 Commissioner Fred F. Fielding of the National Commission on Terrorist Attacks Upon

---

[13] Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003).

[14] *Id*. Admiral Loy stated:

> [w]e are not searching [the National Crime Information Center database] as part of the . . . data that we're looking at . . . . [A]t the moment we are charged with finding in the aviation sector foreign terrorists or those associated with foreign terrorists and keep[ing] them off airplanes. That is our very limited goal at the moment. . . . [E]ven as heinous as it sounds, the axe murderer that gets on the airplane with a clean record in New Orleans and goes to Los Angeles and commits his or her crime, that is not the person we are trying to keep off that airplane at the moment.

[15] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

the United States charged that this expansion of CAPPS II's mission constituted "classic mission creep."[16]

EPIC recommends that DHS recognize US-VISIT's potential for mission creep and work to confine the program to its defined purpose. The vast amount of information contained within US-VISIT makes it an ideal research tool for many purposes. While DHS clearly has a legitimate interest in apprehending suspected terrorists, accused felons, and visitors who overstay their visas, there are innumerable reasons why the agency may want to locate particular individuals who do not fall within these categories. Such uses of US-VISIT data, however, are plainly beyond the authorized scope of US-VISIT's mission of ensuring border security, facilitating trade, and enforcing immigration laws. It is crucial that DHS strictly define the purpose of US-VISIT and limit the use of collected information to its core mission.

Conclusion

For the forgoing reasons, EPIC believes that DHS must give greater consideration to the Privacy Act implications of the system, consider the application of international norms and standards for collection and use of non-U.S. citizens' information as it continues to develop and implement US-VISIT, and not permit mission creep in the program.

Respectfully submitted,

Marc Rotenberg
Executive Director

[16] Panel IV: Risk Management after September 11, Borders, Transportation and Managing Risk, Seventh Public Hearing Before the National Commission on Terrorist Attacks Upon the United States (January 27, 2004).

David Sobel
General Counsel

Marcia Hofmann
Staff Counsel

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009
(202) 483-1140