

DEPARTMENT OF HOMELAND SECURITY
Border and Transportation Directorate

Docket No. DHS-2007-0002

Interim Rule

United States Visitor and Immigrant Status Indicator Technology Program

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published August 31, 2004, the Department of Homeland Security (“DHS”) published an interim rule expanding and further defining the population affected by the United States Visitor and Immigrant Status Indicator Technology (“US-VISIT”) Program.¹ According to the interim rule, US-VISIT is “an integrated, automated entry-exit system that records the arrival and departure of aliens; verifies aliens’ identities; and authenticates aliens’ travel documents through comparison of biometric identifiers.”² The interim rule expands the program to the “50 most highly trafficked land border ports of entry in the United States,” and “further defines the population of aliens who are required to provide biometric identifiers and other identifying information.”³ In response to DHS’s expansion of US-VISIT, the Electronic Privacy Information Center (“EPIC”) calls on the agency to take definite steps to guard against the dangers of mission creep, to take additional factors into account as it determines the effectiveness of the US-VISIT exit pilot programs, and to recognize a right of judicial review for individuals adversely affected by the system.

¹ Interim Rule, 69 Fed. Reg. 53317 (proposed Aug. 31, 2004).

² *Id.* at 53318.

³ *Id.*

Introduction

On January 5, 2004, DHS published an interim rule authorizing the first phase of US-VISIT.⁴ It required travelers using non-immigrant visas to provide “fingerprints, photographs, or other biometric identifiers upon arrival at, or departure from the United States at air and sea ports of entry.”⁵ The program’s entry-exit system is based upon a vast network of databases containing alien arrival and departure data accessible from machine-readable visas, passports and other travel documents.⁶ Since January 5, 2004, aliens entering the U.S. on a nonimmigrant visa at designated air and seaports have been required to submit fingerprints and photographs.⁷ These biometrics are used for identity and background checks.⁸ The information contained within US-VISIT is used not only in furtherance of the program itself, but is also shared with other law enforcement systems.⁹

I. DHS Must Take Measures to Ensure Mission Creep Does Not Occur Within US-VISIT

In its previous comments on US-VISIT, EPIC urged DHS not to expand the use of biometric identifiers beyond the purpose for which they were initially collected.¹⁰ This issue remains critically important because the interim rule reflects DHS’s intention to disclose information maintained within US-VISIT to a broad variety of law enforcement entities whose activities may bear no relationship to US-VISIT’s goals.

According to the US-VISIT Increment 2 Privacy Impact Assessment, US-VISIT collects information about travelers to determine whether an individual:

⁴ Interim Rule, 69 Fed. Reg. 468 (proposed Jan. 5, 2004).

⁵ 69 Fed. Reg. at 53318.

⁶ *Id.* at 53319; 8 U.S.C. § 1731(a)(2) (2004).

⁷ 69 Fed. Reg. at 53320.

⁸ *Id.*

⁹ *Id.* at 53319.

¹⁰ Comments of the Electronic Privacy Information Center, Docket No. BTS 03-01, *available at* http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0440.xml (hereinafter “EPIC Comments”).

- Should be prohibited from entering the U.S.;
- Can receive, extend, change, or adjust immigration status;
- Has overstayed or otherwise violated the terms of their admission;
- Should be apprehended or detained for law enforcement action; and
- Needs special protection/attention (e.g., Refugees).¹¹

According to the interim rule, however, information collected and maintained within US-VISIT could be used for much broader purposes. The interim rule states that US-VISIT information may be disclosed to:

other law enforcement agencies at the federal, state, local, foreign, or tribal level, who, in accordance with their responsibilities, are lawfully engaged in collecting law enforcement intelligence information and/or investigating, prosecuting, enforcing, or implementing civil and/or criminal laws, related rules, regulations, or orders.¹²

The US-VISIT Increment 2 Privacy Impact Assessment explains that such broad “sharing” helps DHS and other law enforcement agencies to “work more cooperatively and effectively in achieving their national security and law enforcement objectives.”¹³ Toward this end, DHS will provide the FBI “direct access” to US-VISIT information with only “Memoranda of Understanding” in place to “minimize any privacy impacts.”¹⁴ Though DHS provides in the interim rule an extensive explanation of the legal basis for US-VISIT, nothing seems to authorize widespread disclosure of data for purposes wholly unrelated to the entry-exit system’s goals.¹⁵

¹¹ Department of Homeland Security, *US-VISIT Program, Increment 2 Privacy Impact Assessment* at 3 (Sept. 14, 2004) at http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_pia_usvisit.pdf.

¹² 69 Fed. Reg. at 53324.

¹³ *US-VISIT Program, Increment 2 Privacy Impact Assessment* at 5.

¹⁴ *Id.*

¹⁵ 69 Fed. Reg. at 53319-53320.

Acknowledging the danger of mission creep within US-VISIT, the interim rule states that “DHS recognizes the importance of privacy rights and will further define the purpose of US-VISIT and the limitations on data collection, maintenance, and use through updates to the Privacy Impact Assessment.”¹⁶ EPIC urges the agency to detail and pursue clear policies on data collection and use limitations in a revised Privacy Impact Assessment as soon as possible. Since January 2003, DHS has been collecting personal information and biometric identifiers of thousands of travelers entering this country every day. Given the extensive “sharing” of US-VISIT information between DHS and other law enforcement entities, there is a high likelihood that this information will be used for purposes beyond the legal authority by which US-VISIT was created.

To further the important objective of guarding against mission creep, EPIC again 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 that all individuals have rights in their personal information, regardless of nationality. As discussed in EPIC’s previous comments, US-VISIT’s collection and use of personal information of non-U.S. citizens violates the principles of the OECD Privacy Guidelines of 1980,¹⁷ the United Nations Guidelines for the Regulation of Computerized Personal Files of 1990,¹⁸ the European Union Data Protection Directive,¹⁹ and the Universal Declaration of Human Rights,²⁰ to which the

¹⁶ 69 Fed. Reg. at 53324.

¹⁷ 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 M. ROTENBERG ED., THE PRIVACY LAW SOURCEBOOK 2003, 330 (EPIC 2003) (hereinafter “PRIVACY LAW SOURCEBOOK”).

¹⁸ 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.

¹⁹ Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with

United States is an original signatory.²¹ A number of countries, including Brazil, Japan, and China,²² have objected to DHS's collection and use of biometric and personal information about their citizens. As it expands US-VISIT, DHS should recognize the danger of continuing to disregard international human rights standards, and strive to align its practices with the principles articulated by international guidelines for protecting privacy.

As a final matter, EPIC commends DHS's expressed commitment to continually evaluate the need to store certain types of data and adjust the system accordingly.²³ However, EPIC reiterates the importance of retaining only the information absolutely necessary to carry out the narrow objectives of the program.

II. DHS Must Evaluate the Accuracy and Security Implications of the US-VISIT Exit Pilot Programs

DHS has implemented US-VISIT exit pilot programs at Baltimore-Washington International Airport and the Miami Seaport, which are testing different methods of processing to determine "the most accurate and efficient collection of information from aliens departing from the United States."²⁴ These programs implement several methods of data collection, including self-serve kiosks and hand-held scanners.²⁵ According to the interim rule, the programs will be evaluated based on:

Regard to the Processing of Personal Data and on the Free Movement of Such Data, reprinted in PRIVACY LAW SOURCEBOOK at 371.

²⁰ 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 PRIVACY LAW SOURCEBOOK at 318.

²¹ EPIC Comments, *supra* at 3-4.

²² See Larry Rohter, *Brazil Seeks to Bypass Fingerprinting*, NY Times, Jan. 14, 2004, at A9; *Japan to Demand U.S. Erase Fingerprints, Photos After Visitors Leave Country*, Mainichi Daily News, Sept. 29, 2004, available at <http://www12.mainichi.co.jp/news/mdn/search-news/916107/US2dVISIT-0-1.html>; *FM: US Urged Not to Fingerprint Chinese*, ChinaDaily.com, March 24, 2004, available at http://www.chinadaily.com.cn/english/doc/2004-03/24/content_317687.htm.

²³ 69 Fed. Reg. at 53324.

²⁴ *Id.* at 53320.

²⁵ *Id.*

(1) The cost of each option, including the impact on staffing and necessary personnel; (2) how well the alternative supports all necessary aliens being processed and requisite law enforcement functions; and (3) how conducive the alternative is for tourist and commercial travel.²⁶

It is hard to imagine how the “most accurate and efficient” system can be determined by this set of criteria without any consideration of the rate of error associated with each system. Use of biometrics carries a risk of misidentification — both false positives and false negatives.²⁷ DHS should also consider the systems’ accuracies as the agency evaluates the best way to collect such data.

The interim rule also suggests that DHS is not considering security concerns as part of its evaluation. A large database containing personal information along with biometric identifiers is always subject to dangers of abuse, unauthorized access, and mission creep. DHS has stated a commitment to protecting the privacy interests of those affected by US-VISIT. It is important for the agency to follow through on this commitment by ensuring that its methods of biometric data collection are secure.

III. DHS Should Recognize a Right of Judicial Review For Individuals Adversely Affected by US-VISIT

EPIC commends DHS for its decision to establish a three-step redress process through which individuals may dispute the accuracy of information contained within the US-VISIT system.²⁸ EPIC notes that the Privacy Act of 1974 provides rights to access and correct information only to U.S. citizens and permanent residents, and that individuals subject to US-VISIT generally do not have such rights under the law.²⁹

However, in the interest of creating the most privacy-friendly system possible, EPIC

²⁶ *Id.* at 53321.

²⁷ See generally Electronic Privacy Information Center, *Biometric Identifiers*, at <http://www.epic.org/privacy/biometrics> (last updated March 30, 2004).

²⁸ 69 Fed. Reg. at 53332-53333.

²⁹ 5 U.S.C. § 552a(a)(2).

strongly urges DHS to consider providing a right to judicial review if an individual affected by US-VISIT finds the appeals process established by DHS unsatisfactory. A determination using US-VISIT information can have an immense impact on the lives of those subject to the system. Non-immigrant visitors may not have rights consistent with those provided by the Privacy Act, but ideally should have an avenue of appeal to a third party independent of the agency responsible for maintaining the system.

Conclusion

For the foregoing reasons, EPIC believes that DHS, in its continued implementation of US-VISIT, must further protect against the dangers of mission creep, evaluate the accuracy and security of its pilot program, and recognize a right of judicial review for individuals adversely affected by the program.

Respectfully submitted,

Marc Rotenberg
Executive Director

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel

Paul Jones
IPIOP Law Clerk

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