

DEPARTMENT OF HOMELAND SECURITY
United States Customs and Border Protection

Docket No. DHS-2005-0053
Notice of Revision to and Expansion of Privacy Act System of Records

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on April 21, 2006, United States Customs and Border Protection (“CBP”) announced “a revision to and expansion of a previously-established Privacy Act system of records, the Global Enrollment System.”¹ CBP seeks this revision and expansion “to facilitate the creation of a consolidated database to collect biometric and biographic data for individuals who voluntarily exchange personally identifiable information in return for expedited transit at U.S. border entry points.”² CBP also seeks to exempt this system from several significant provisions of the Privacy Act of 1974.³

This system will cover all individuals who “apply to use any form of automated or other expedited inspection for verifying eligibility to cross the borders into the United States.”⁴ Among many possible activities, the CBP will use this system to determine which travelers will be eligible for the “Trusted Traveler” program and to make decisions that will therefore directly impact which citizens are deemed by the government to be “low-risk” travelers and which travelers would be subject to enhanced screening procedures.

Pursuant to this CPB notice, the Electronic Privacy Information Center (“EPIC”) submits these comments to address the substantial privacy and security issues raised by

¹ Privacy Act Notice, 71 Fed. Reg. 20708 (Apr. 21, 2006).

² *Id.*

³ *Id.* at 20710.

⁴ *Id.* at 20709.

the database and to request that CBP substantially narrow the Privacy Act exemptions in the notice prior to the revision and expansion of this system of records.

Introduction

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.⁵ The Supreme Court just two years ago underscored the importance of the Privacy Act’s restrictions upon agency use of personal information to protect privacy interests, noting that:

“[I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies.” Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government’s part to comply with the requirements.⁶

The Privacy Act is intended “to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]”⁷ It is also intended to guard the privacy interests of citizens and lawful permanent residents 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 personal and fundamental right protected by the Constitution of the United States.”⁸ It thus sought to

⁵ S. Rep. No. 93-1183 at 1 (1974).

⁶ *Doe v. Chao*, 540 U.S. 614, 618 (2004).

⁷ S. Rep. No. 93-1183 at 1.

⁸ Pub. L. No. 93-579 (1974).

“provide certain protections for an individual against an invasion of personal privacy” by establishing a set of procedural and substantive rights.⁹

Adherence to these requirements is critical for a system such as the Global Enrollment System (“GES”), a massive centralized repository of data that would include:

[D]ata such as full name, including nickname or other names used, place and date of birth, gender, current and former addresses, telephone numbers, country of citizenship, alien registration number (if applicable), employment history, biometric data, driver's license number and issuing state or province, the make, model, color, year, license number and license issuing state or province of the applicant's vehicle, the flag and home port (where the vessel is foreign flagged), name, registration number and registration issuing state or province of the applicant's vessel, the name and address of the vehicle's or vessel's registered owners if different from the applicant, and the amount of fee paid. The application may also include such information as the frequency of border crossings or travel, and the most frequent reason for crossing the border or travel, information supplied by the applicant as to whether he or she has been arrested or convicted of any violations of law, and information obtained from checks of other law enforcement databases that would confirm or refute this information.¹⁰

This data would be maintained in a computer database at the CBP National Data Center in Washington, DC and would be available through terminals that are accessible at border ports of entry and airports and seaport inspection facilities under the jurisdiction of the Department of Homeland Security.¹¹

As CBP notes in the Federal Register Notice, the Privacy Act “embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates personally identifiable information.”¹² Unfortunately, the CBP proposes to exempt the GES from key fair information principles such as the requirements that an individual be permitted access to

⁹ *Id.*

¹⁰ 71 Fed. Reg. at 20709-10.

¹¹ *Id.* at 20709.

¹² *Id.* at 20709.

personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use.¹³ It is clear that this sweeping new system of records is precisely the type of database that requires application of these principles as embodied in the Privacy Act.

I. The Global Enrollment System’s Broad Exemptions Contravene the Intent of the Privacy Act

As an initial matter, we note that CBP has invoked 5 U.S.C. §§ 552a(j)(2) and (k)(2) as authority for its exemption of specific Privacy Act requirements. These broad exemptions would allow CBP to create and use this massive database with little accountability.

Customs and Border Protection claims subsection (j)(2) exemptions from 5 U.S.C. §§ 552a(e)(8) and (g). Subsection (e)(8) mandates that the agency “make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.”¹⁴ If the process is a “matter of public record,” it is unknown what value would be gained by exempting the agency from its Privacy Act obligation to make reasonable efforts to serve notice on an affected individual. This broad exception only serves to increase the secrecy of the database.

Subsection (g) specifies the civil remedies that an individual has against an agency for failure to comply with its obligations under the Privacy Act. Exempting GES from subsection (g) of the Privacy Act means that individuals will have no judicially

¹³ See U.S. Dep’t of Health, Education and Welfare, *Secretary’s Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* viii (1973).

¹⁴ 5 U.S.C. § 552(a)(e)(8).

enforceable rights of access to their records or correction of erroneous information in such records.

In its notice, CBP has exempted GES from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;¹⁵
- an individual may seek judicial review to enforce the statutory right of access provided by the Act,¹⁶ and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.¹⁷

In lieu of the statutory, judicially enforceable right of access provided by the Act, CBP creates an administrative right of access and redress through its records access procedures.¹⁸ For redress, a person must write to CBP Customer Satisfaction Unit in the Office of Field Operations or the DHS Director for Departmental Disclosure and FOIA. While we commend CBP for creating a redress process, it is a weak one, at best. This conflicts with the purposes of the Privacy Act, which intended to provide an enforceable right of access to personal information maintained by government agencies. As then-DHS Privacy Officer Nuala O'Connor Kelly testified before Congress in February 2004, "Issues of privacy and civil liberties are most successfully navigated when the necessary legal, policy, and technological protections are built in to the systems or programs from the very beginning."¹⁹ The Global Enrollment System should include a strong framework

¹⁵ 5 U.S.C. § 552a(d)(1).

¹⁶ 5 U.S.C. § 552a(g)(1).

¹⁷ 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).

¹⁸ 71 Fed. Reg. at 20710.

¹⁹ Statement of Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Before the House of Representatives Judiciary Subcommittee on Commercial

for privacy and civil liberties.

The Department of Homeland Security's redress procedures have largely been inadequate. For example, the Transportation Security Administration ("TSA") maintains that it has an adequate redress process to clear individuals improperly flagged by watch lists; however, it is well known that individuals encounter difficulty in resolving such problems. Senators Ted Kennedy (D-MA) and Don Young (R-AK) are among the individuals who have been improperly flagged by watch lists.²⁰ Sen. Kennedy was able to resolve the situation only by enlisting the help of then-Homeland Security Secretary Tom Ridge; unfortunately, most people do not have that option.

The massive size of the terror watch lists, recently revealed to include 325,000 names, merely underscores this "false positive" problem.²¹ TSA also does not include a judicially enforceable right of redress. TSA and CBP's failure to include this protection reduces the opportunity for individuals to correct records, and thereby increases the likelihood of mistakes. Such errors distract officials, who could be focusing on those who are linked to terrorist activity.

Providing individuals with the right to judicial review is crucial because the database will have information not only proffered by individuals, but also gathered from

and Administrative Law (Feb. 10, 2004) at http://www.dhs.gov/dhspublic/interapp/testimony/testimony_0024.xml (last accessed May 22, 2006).

²⁰ See, e.g., Sara Kehaulani Goo, *Committee Chairman Runs Into Watch-List Problem*, Washington Post, Sept. 30, 2004; Leslie Miller, *House Transportation Panel Chairman Latest to be Stuck on No-Fly List*, Associated Press, Sept. 29, 2004; Shaun Waterman, *Senator Gets a Taste of No-Fly List Problems*, United Press International, Aug. 20, 2004.

²¹ Walter Pincus and Dan Eggen, *325,000 Names on Terrorism List*, Washington Post, Feb. 15, 2006.

other sources, including law enforcement databases.²² It is also important because regulations for the retention or disposal of information gathered for this database is unknown. Under the previous system, records were “destroyed three years after the denial of an application as a ‘trusted traveler’ or after an issued permit expires.”²³ Under the revised and expanded GES, CBP has said, “In light of the changes to the program that are envisioned, CBP will work with its Records personnel to develop an appropriate retention schedule that accounts for both operational and privacy concerns.”²⁴ CBP has not explained why it did not include draft regulations for retention and disposal in this Privacy Act notice, though it included other revisions and expansions of GES.

Though section (j) requires an agency to provide the “reasons why the system of records is to be exempted from a provision of this section,” CBP does not explain why it has exempted GES from these Privacy Act requirements. CBP also cites subsection (k)(2) in support of these exemptions. Subsection (k)(2) is applicable only where the system of records is “investigatory material compiled for law enforcement purposes.” The subsection provides, however, that “if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual.” Given that CBP seeks to exempt GES from the Privacy Act’s access provisions, it is unclear whether subsection (k)(2) authorizes CBP action. As such, we urge CBP to explain how (k)(2) gives the agency authority to exempt the system of records from the various Privacy Act provisions it cites.

²² 71 Fed. Reg. at 20709-10.

²³ *Id.* at 20710.

²⁴ *Id.*

II. The Global Enrollment System's Trusted Traveler Program Creates a Significant Security Risk

Customs and Border Protection is revising and expanding GES in order “to perform advanced screening on low-risk trusted travelers and to expedite the security screening process of these trusted travelers as their low-risk status is confirmed.”²⁵

However, this “Trusted Traveler” system creates a substantial security risk, as it divides travelers into categories whose criteria can be learned and exploited.

The program creates two classes of travelers: trusted and not trusted. But, as security expert Bruce Schneier has explained, this could also create a third category: “bad guys with the card.”²⁶ Criminals will choose applicants without previous links to terrorism, who can pass the background checks, to commit their crimes. For example, neither Oklahoma City bomber Timothy McVeigh nor Unabomber Ted Kaczynski had previous ties to terrorism, Schneier said.²⁷

There are a number of approaches to this problem, none of which are considered by the CBP in its proposed expansion of the Global Enrollment System. First, the best procedure may be to subject all travelers to the security screening that would be required for a suspicious traveler. Second, if the Trusted Traveler program is adopted, it may be necessary to include random security screenings even for those passengers who have been designated “low-risk” travelers so that those who obtain such a designation but intend harm will still be at risk of more thorough security screening. Third, as EPIC has previously recommended, the best approach may be to focus on security techniques that

²⁵ *Id.* at 20709.

²⁶ Bruce Schneier, *Crypto-Gram Newsletter*, Mar. 15, 2004, at <http://www.schneier.com/crypto-gram-0403.html>.

²⁷ *Id.*

are intended to detect devices and other materials that may threaten air travel safety rather than profiling techniques that attempt to divine the intent of travelers.²⁸ One obvious problem with a security protocol that is based on a distinction between “low-risk” and “high-risk” traveler is that a “high-risk” traveler may exploit the status of the “low-risk” traveler to enable the delivery of dangerous materials to the aircraft.²⁹ This is a further reason that the expansion of databases that are intended to promote profile-based security determinations should be viewed with some skepticism.

III. The Global Enrollment System’s Presents a High Risk of Mission Creep

The Global Enrollment System’s many categories of “routine uses” creates a strong risk of “mission creep.” This is a risk that information volunteered will be used for reasons not related to their original security purposes.

“Trusted Traveler” applicants must submit a substantial amount of personally identifiable information, including biometric data and employment history. This personal information could be used for reasons other than the ones for which the information was gathered or volunteered. In this program, CBP has identified seven categories of “routine uses” of personal information that will be collected and maintained in the program’s system of records. In one category, CBP anticipates disclosure to:

²⁸ Prepared Testimony and Statement for the Record of Marc Rotenberg, President, Electronic Privacy Information Center, at a Hearing on Security and Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States (Dec. 8, 2003), *available at* <http://www.epic.org/privacy/terrorism/911commtest.pdf>.

²⁹ Prepared Testimony and Statement for the Record of Marc Rotenberg, President, Electronic Privacy Information Center, at a Hearing on the Future of Registered Traveler Before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the U.S. House of Representatives Committee on Homeland Security (Nov. 3, 2005), *available at* http://www.epic.org/privacy/airtravel/rt_test_110305.pdf.

Federal, State, local, foreign, international or tribal government agencies or organizations that are lawfully engaged in collecting intelligence or law enforcement information (whether civil, criminal or administrative) and/or charged with investigating, prosecuting, enforcing or implementing civil and/or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement and intelligence responsibilities.³⁰

This category is so broad as to be almost meaningless, allowing for potential disclosure to virtually any government agency worldwide for a vast array of actual or “potential” undefined violations. The risk of mission creep is clear.

Conclusion

For the foregoing reasons, the Electronic Privacy Information Center believes that CBP must revise its Privacy Act notice for the Global Enrollment System to 1) provide individuals judicially enforceable rights of access and correction; 2) create suitable retention and disposal standards; 3) limit the distribution of information to only those necessary for the screening process; and 4) respect individuals’ rights to their information that is collected and maintained by the agency.

Respectfully submitted,

Marc Rotenberg
Executive Director

Melissa Ngo
Staff Counsel

³⁰ 71 Fed. Reg. at 20710.

ELECTRONIC PRIVACY INFORMATION
CENTER

1718 Connecticut Avenue, N.W.

Suite 200

Washington, DC 20009

(202) 483-1140