COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
UNITED STATES CUSTOMS AND BORDER PROTECTION; DEPARTMENT OF HOMELAND SECURITY

"Establishment of Global Entry Program"

Docket No. USCBP-2008-0097

January 19, 2010

By notice published on November 19, 2009, United States Customs and Border Protection ("CBP") announced that it is "proposing to amend its regulations to establish Global Entry as a permanent international trusted traveler program."[1]

Pursuant to the CBP notice in the Federal Register, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy and security issues raised by the Global Entry program. EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has particular interest in preserving privacy safeguards in the development of new information systems and new procedures for identity management.[2]

---

[1] Establishment of Global Entry Program, 74 Fed. Reg. 59932 (Nov. 19, 2009) (to be codified at 8 C.F.R. pts. 103 and 235).

[2] *See* EPIC: Air Travel Privacy, http://epic.org/privacy/airtravel; EPIC: Biometric Identifiers, http://epic.org/privacy/biometrics; EPIC: Automated Targeting System, http://epic.org/privacy/travel/ats/default.html; EPIC: Whole Body Imaging, http://epic.org/privacy/airtravel/backscatter; EPIC: Spotlight on Surveillance – Registered Traveler Card, http://epic.org/privacy/surveillance/spotlight/1005; EPIC: Secure Flight, http://epic.org/privacy/airtravel/secureflight.html.

Scope of Rulemaking

CBP seeks to make the program permanent in order to "facilitate the movement of low-risk, frequent air travelers arriving from outside the United States."[3] CBP states that Global Entry "will provide an expedited inspection and examination process for pre-approved, pre-screened travelers by allowing them to proceed directly to automated Global Entry kiosks upon their arrival in the United States."[4]

Global Entry was first activated by the CBP on June 6, 2008, as a pilot program in seven airports. On August 24, 2009, CBP expanded the pilot program to 13 other airports.[5]

Under the program, international travelers may register with the CBP by providing their passport information and a copy of their fingerprints.[6] According to CBP, registrants must also pass a background check and an interview with a CBP officer before they may be enrolled in the program.[7] Only individuals who are 14 years of age and older who are U.S. citizens, U.S. nationals, U.S. Lawful Permanent Residents, or citizens of certain other countries may enroll in Global Entry.[8] Individuals may be disqualified from enrolling if they:

- Are inadmissible to the United States under applicable immigration laws;
- Provide false or incomplete information on their application;
- Have been convicted of a criminal offense in any country;
- Have been found in violation of customs or immigration laws; or

---

[3] *Id.* at 59933.
[4] *Id.*
[5] Press Release, Department of Homeland Security, Secretary Napolitano Announces Global Entry Expansion to 13 Additional Airports (Aug. 12, 2009), *available at* http://www.dhs.gov/ynews/releases/pr_1250094008914.shtm.
[6] Department of Homeland Security, Global Entry Program Overview, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry/global_entry_discription.xml (last visited Jan. 19, 2010).
[7] *Id.*
[8] *Id.*

- Fail to meet other Global Entry requirements.[9]

Registered international travelers can then bypass conventional airport security lines by scanning their passports and fingerprints at a kiosk, answering customs declaration questions, and then presenting a receipt to Customs officials.[10]

According to CBP, the information collected through the on-line application is deposited into the Global Enrollment System (GES), a system of records for CBP trusted traveler programs.[11] CBP can share applicants' personal information, including fingerprint biometrics, with other government and law enforcement agencies. CBP stores applicants' information in two separate systems of records: "personal information" is stored in the GES, and "applicant biometrics" are stored in the Department of Homeland Security (DHS) Automated Biometric Identification System, or IDENT.

EPIC's Comments and Recommendations

1. Global Entry Contravenes the Intent of the Privacy Act

Global Entry stores applicants' personal information in the GES. However, the GES, a sweeping system of records, invokes broad exemptions from the Privacy Act that would allow CBP to augment the massive database and use the information with little accountability.

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.[12] The Supreme Court recently underscored the importance of the Privacy Act's restrictions upon agency use of personal information to protect privacy interests, noting that:

---

[9] *Id.*
[10] *Id.*
[11] Establishment of Global Entry Program, 74 Fed. Reg. at 59938.
[12] S. Rep. No. 93-1183 at 1 (1974).

> "[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.[13]

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[.]"[14] 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."[15] 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.[16]

The GES, when created in 2006, exempted the GES from key fair information practices such as the requirements that an individual be permitted access to 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.[17] Those exemptions remain, and the

[13] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[14] S. Rep. No. 93-1183 at 1.
[15] Pub. L. No. 93-579 (1974).
[16] *Id.*
[17] *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).

Global Entry information stored in the GES is subject to the same problems caused by those exemptions.

At the time, CBP invoked 5 U.S.C. §§ 552a(j)(2) and (k)(2) as authority for its exemption from specific Privacy Act requirements. Customs and Border Protection claimed 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."[18] If the process is a "matter of public record," it is unclear what value would be gained from 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 participating in Global Entry will have no judicially enforceable rights of access to their records or correction of erroneous information in such records.

CBP also 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[19]; an individual may seek judicial review to enforce the statutory right of access provided by the Act[20]; and the agency must publish a notice of the existence of records in the Federal Register,

[18] 5 U.S.C. § 552(a)(e)(8).
[19] 5 U.S.C. § 552a(d)(1).
[20] 5 U.S.C. § 552a(g)(1).

along with the procedures to be followed to obtain access.[21] In lieu of the statutory, judicially enforceable right of access provided by the Act, CBP created an administrative right of access and redress through its records access procedures.[22] 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. The redress process is a weak one, at best, and 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."[23] The Global Enrollment System and the Global Entry information stored therein should include a strong framework for privacy and civil liberties.

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 other sources, including law enforcement databases.[24] 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."[25] Under the revised and expanded GES, CBP said, "In light of the changes to the program that are envisioned, CBP will work with its Records personnel to

[21] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[22] Privacy Act Notice, 71 Fed. Reg. 20708, 20710 (Apr. 21, 2006).
[23] Statement of Nuala O'Connor Kelly, Chief Privacy Officer, Department of Homeland Security, Before the House of Representatives Judiciary Subcommittee on Commercial Comments of and Administrative Law (Feb. 10, 2004).
[24] 71 Fed. Reg. at 20709-10.
[25] *Id*. at 20710.

develop an appropriate retention schedule that accounts for both operational and privacy concerns."[26] CBP did not explain why it did not include draft regulations for retention and disposal at the time, though it included other revisions and expansions of GES.

For the foregoing reasons, EPIC submitted comments to CBP in 2006 regarding the GES system of records, arguing that the database raises substantial privacy and security issues, and requesting that CBP narrow its claimed exceptions from the Privacy Act of 1974.[27] By placing the data of Global Entry applicants into the GES system of records, CBP is expanding a flawed system and failing to protect individuals' privacy.

2. Global Entry Creates a Significant Security Risk

The Global Entry program also repeats the failures of past "trusted traveler" programs. A trusted traveler system creates substantial security risks, as it divides travelers into categories whose criteria can be learned and exploited: trusted and not trusted. But, as security expert Bruce Schneier has explained, this could also create a third category: "bad guys with the card."[28] 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.

The inclusion of Global Entry data into the GES system of records also increases the risk of "mission creep." This is a risk that information volunteered will be used for reasons not related to their original security purposes. Global Entry applicants must submit a substantial amount of personally identifiable information, including biometric data and employment history.

---

[26] *Id*.

[27] Comments of the Electronic Privacy Information Center, Privacy Act Notice, 71 Fed. Reg. 20708 (Feb. 20, 2007), *available at* http://epic.org/privacy/airtravel/ges052206.pdf.

[28] Bruce Schneier, *"I am Not a Terrorist" Cards*, Crypto-Gram Newsletter, Mar. 15, 2004, http://www.schneier.com/crypto-gram-0403.html#10 (last visited Jan. 19, 2010).

This personal information could be used for reasons other than the ones for which the information was gathered or volunteered. The GES system of records, in which the Global Entry information will be stored, identifies seven categories of "routine uses" of personal information that will be collected and maintained in the program's system of records.[29] In one category, CBP anticipates disclosure to:

> 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.

3. The CBP Failed to Conduct a Privacy Impact Assessment

Global Entry stores applicants' personal information in the GES. However, CBP did not even conduct a privacy impact assessment regarding Global Entry. Instead, CBP's Federal Register notice simply refers to the Privacy Act notice and Privacy Impact Assessments (PIA) issued when the GES was created. CBP should have conducted an independent analysis of the privacy impact of Global Entry.

PIAs are of paramount importance and are mandated by federal law. Under the E-Government Act of 2002, a federal government agency *must* conduct a PIA under the following circumstances:

> before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii)

[29] 71 Fed. Reg. at 20710.
[30] *Id.*

> initiating a new collection of information that—(I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

E-Government Act of 2002 § 208(b)(1)(A), 44 U.S.C. § 3501 (2008). Once those conditions are triggered, the agency is required to conduct a PIA:

> Each agency *shall (i) conduct a privacy impact assessment*; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

Id. § 208(b)(1)(B) (emphasis added). Indeed, DHS acknowledges that it is required to conduct a PIA "for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information." The Privacy Office, Department of Homeland Security, Privacy Impact Assessments: Official Guidance 5 (2007). DHS thus states that "[a] PIA should be completed for any program, system, technology, or rulemaking that involves personally identifiable information."

The establishment of the Global Entry program meets the conditions that trigger CBP's obligation to conduct a PIA *before* developing or initiating the program. Global Entry is a system that involves personally identifiable information. That information will be "collected, maintained, or disseminated using information technology." There is no indication that CBP conducted a PIA regarding Global Entry. The Federal Register notice for the program states the following regarding privacy and PIAs:

> The on-line application for Global Entry collects information similar to that collected on applications for CBP's other trusted traveler programs (e.g., NEXUS, SENTRI and FAST). The information collected through the on-line application is deposited into the Global Enrollment System (GES), as the system of record for

> CBP trusted traveler programs. The personal information provided by the applicants, including the fingerprint biometrics taken at the time of the personal interview, may be shared with other government and law enforcement agencies in accordance with applicable laws and regulations. The personal information that is collected through GOES is maintained in a Privacy Act system of records (GES) that was last published in the Federal Register (71 FR 20708) on April 21, 2006. CBP has also published two Privacy Impact Assessments that cover this program on the DHS Privacy Office Web site, http://www.dhs.gov/privacy [GES, GOES]. In addition, an update addressing on-line functionality of the enrollment process was posted to the DHS Privacy Office Web site on November 1, 2006.

It is insufficient for CBP to simply refer to the PIAs it conducted regarding GES and GOES. Global Entry is a separate system that involves the collection, maintenance and dissemination of separate personally identifiable information. Thus, federal law required CBP to conduct a PIA *before* developing or initiating the program

In addition to the federal statutory mandate to conduct the PIA, the Department of Homeland Security's official guidance on PIAs highlights the paramount importance of conducting PIAs on systems like Global Entry:

> The [PIA] is one of the most important instruments through which the Department establishes public trust in its operations. . . . The PIA is a vital tool that evaluates possible privacy risks and the mitigation of those risks at the beginning of and throughout the development life cycle of a program or system. The transparency and analysis of privacy issues provided by a PIA demonstrates that the Department actively engages program managers and system owners on the mitigation of potential privacy risks.

The Privacy Office, Department of Homeland Security, Privacy Impact Assessments: Official Guidance 2 (2007). CBP should undertake a PIA before proposing to permanently establish Global Entry.

4. CBP Should Consider Past Failures with the "Clear" Registered Traveler Program

The lessons learned from the Clear registered traveler program weigh against the establishment of any registered traveler program. Clear, which was operated by Verified Identity Pass, a private company, was the largest registered traveler program in the nation, operating out

of 20 airports with roughly 165,000 members. The Transportation Security Administration (TSA) established registered traveler security, privacy, and compliance standards for the Clear program and bolstered the company's credentials with the traveling public.[31] The Clear program's application process collected a great deal of personal information from members, such as proof of legal name, data of birth, citizenship status, home address, place of birth, and gender. The information was used to pre-screen travelers for express service through airport security checkpoints. However, the program encountered several problems. First, it suffered a security breach when a laptop containing the personal information of roughly 33,000 travelers was stolen. As a result, TSA suspended new applications to the program.[32] Subsequently, Verified Identity Pass declared its intent to declare bankruptcy, leading the House Homeland Security Committee to investigate when the TSA became aware of the bankruptcy; whether they asked the company for its plan regarding its registered traveler data; whether the agency sought a privacy impact assessment on the bankruptcy; and whether the agency had a contingency plan for safeguarding the data after the company went out of business.[33]

The concerns expressed by the TSA and by the House Homeland Security Committee underscore the sensitivity of the information collected by Clear—information that would also be collected under the Global Entry program. At minimum, the lessons learned from Clear

[31] *See* Transportation Security Administration, Registered Traveler, July 15, 2009, http://www.tsa.gov/approach/rt/index.shtm.

[32] Press Release, Transportation Security Administration, TSA Suspends Verified Identity Pass, Inc. Clear Registered Traveler Enrollment (Aug. 4, 2008), *available at* http://www.tsa.dhs.gov/press/releases/2008/0804.shtm.

[33] Letter from House Committee on Homeland Security to Gale Rossides, Acting Assistant Secretary, Transportation Security Administration (June 25, 2009), *available a*t http://epic.org/dhs-committee_tsa-ltr.pdf.

reemphasize the need for a separate PIA regarding Global Entry and a reassessment of its security and privacy implications.

Conclusion

For the foregoing reasons, the Electronic Privacy Information Center urges CBP to revise its establishment of the Global Entry program and to reconsider the privacy and security implications of the program. Global Entry should 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. Moreover, the agency should undertake a Privacy Impact Assessment, particularly in light of the fiasco encountered under Clear, a similar registered traveler program.

Respectfully submitted,

/s/
Marc Rotenberg
Executive Director

Matthew Phillips
Appellate Advocacy Counsel