DEPARTMENT OF HOMELAND SECURITY
United States Customs and Border Protection

Docket No. DH6-2006-0060
Notice of Privacy Act System of Records

COMMENTS OF 30 ORGANIZATIONS AND 16 EXPERTS IN PRIVACY AND TECHNOLOGY

URGING THE DEPARTMENT OF HOMELAND SECURITY TO

(A) SUSPEND THE "AUTOMATED TARGETING SYSTEM" AS APPLIED TO INDIVIDUALS, OR IN THE ALTERNATIVE, (B) FULLY APPLY ALL PRIVACY ACT SAFEGUARDS TO ANY PERSON SUBJECT TO THE AUTOMATED TARGETING SYSTEM

By notice published on November 2, 2006, United States Customs and Border Protection ("CBP") purports to "provide expanded notice and transparency to the public" regarding the Automated Targeting System ("ATS").[1] CBP claims that, "this system of records notice does not identify or create any new collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems."[2] CBP also seeks to exempt the ATS from several significant provisions of the Privacy Act of 1974.[3] Pursuant to this CPB notice, the 30 organizations and 16 experts in privacy and technology listed below submit these comments to address the substantial privacy and security issues raised by the database, to urge that the CBP cease retaining personal information on American citizens in the ATS, and to demand that CBP significantly narrow the Privacy Act exemptions for the system if the proposal goes forward.

---

[1] Department of Homeland Security, *Notice of Privacy Act system of records*, 71 Fed. Reg. 64543 (Nov. 2, 2006).
[2] *Id*.
[3] *Id*. at 64545.

The Automated Targeting System was created to screen shipping cargo. Although there is some ambiguity as to when the DHS first began to create "terrorist profiles" for American travelers, in this Privacy Act System of Records Notice, the CBP is now admitting that, without adequate notice and in violation of the Privacy Act, it has been using the ATS to conduct background checks on tens of millions of travelers and to assign secret terrorist ratings on US citizens. The resulting "risk assessments" will determine whether individuals will be subject to invasive searches of their persons or belongings, and whether U.S. citizens will be permitted to enter or exit the country. As the agency notice makes clear, the ATS profiles may be integrated with other government databases and may be used for a wide variety of purposes.

The current use of ATS for profiling and storage purposes should be suspended immediately, for it is being conducted in clear violation of the Privacy Act, having not been the subject of a proper system of records notice or a Privacy Impact Assessment. (A Privacy Impact Assessment was issued on November 22 of this year, too late to have any relevance to the decisions about how to use ATS that are reflected in this notice). Throughout these comments, we will treat the application of ATS to individuals as a secret government program that was undertaken in violation of the federal Privacy Act. As such, the presumption would be to suspend the program until the formal requirements of the Privacy Act are satisfied. We further urge DHS to examine not only the Privacy Act requirements for a system of records established by a federal agency, but also the fundamental question of efficacy and resource allocation posed by the creation of a massive database established to profile American citizens that lacks any effective means of oversight or evaluation.

If the CBP proposal as described in the Privacy Act notice goes forward, the profiles will be widely accessible across the federal government. However, individuals will not have judicially enforceable rights to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. It is precisely the kind of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.[4]

Introduction

The agency proposes that the ATS, which was created to screen shipping cargo, be extended so that it would scrutinize all people "seeking to enter or exit the United States," "engag[ing] in any form of trade or other commercial transaction related to the importation or exportation of merchandise," "employed in any capacity related to the transit of merchandise intended to cross the United States border," and "serv[ing] as operators, crew, or passengers on any vessel, vehicle, aircraft, or train who enters or exits the United States."[5] This is an extraordinary change and precisely the type of mission creep that has been of concern to the public and the Congress with respect to the systems established by the Department of Homeland Security. It affects an extraordinary number of people. In Fiscal Year 2005, Customs and Border Protection "processed 431 million pedestrians and passengers, 121 million privately owned vehicles, and processed and cleared 25.3 million sea, rail, and truck containers."[6]

---

[4] 5 U.S.C. § 552a.
[5] 71 Fed. Reg. at 64544.
[6] W. Ralph Basham, Commissioner, Customs and Border Protection, Department of Homeland Security, *Statement at a Hearing on Customs Budget Authorizations & Other Customs Issues Before the Subcom. on Trade of the H. Comm. on Ways & Means*, 109th Cong. (July 25, 2006) *available at* http://waysandmeans.house.gov/hearings.asp?formmode=view&id=5160.

The November 2, 2006 system of records notice on ATS claims it "is providing additional notice and transparency of the functionality of these systems," but there was no notice or transparency before ATS began screening U.S. citizens, not just shipping cargo.[7] As recently as March, ATS was described as "a computerized model that CBP officers use as a decision support tool to help them target oceangoing cargo containers for inspection."[8] Also, there is a lack of public information on the manner in which ATS will assess the security risks particular individuals are deemed to pose.

The agency notice states that the:

> ATS builds a risk assessment for cargo, conveyances, and travelers based on criteria and rules developed by CBP. ATS maintains the resulting [secret] assessment together with a record which [secret] rules were used to develop the [secret] assessment. . . . This assessment and related rules history associated with developing a [secret] risk assessment for an individual are maintained for up to forty years to support ongoing [secret] targeting activities. (emphasis added).

As the bracketed comments indicate, all of the key characteristics of the system – including the assessment, the basis for the assessment, the rules that apply, and the "targeting activities" – are secret. The agency has, in effect, proposed the establishment of a massive black box with detailed profiles, ratings, and targeting rules concerning US citizens that will be widely accessible across the federal government and may be used for a wide variety of agency activities but will not be available to the person about whom decisions will be made. This is not transparency.

---

[7] 71 Fed. Reg. at 64543.

[8] Richard M. Stana, Director, Homeland Security and Justice Issues, Government Accountability Office, *Testimony at a Hearing on Neutralizing the Nuclear and Radiological Threat: Securing the Global Supply Chain (Part Two) Before the Subcom. on Investigations of the S. Comm. on Homeland Security and Governmental Affairs*, 109th Cong. (Mar. 30, 2006) [hereinafter "GAO Testimony on ATS"] *available at* http://www.gao.gov/new.items/d06591t.pdf.

When it enacted the Privacy Act in 1974, Congress sought to make government agencies accountable for the information they collected on US citizens and required agencies to be transparent in their information practices.[9] 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.[10]

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[.]"[11] 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."[12] 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.[13]

---

[9] S. Rep. No. 93-1183 at 1 (1974).
[10] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[11] S. Rep. No. 93-1183 at 1.
[12] Pub. L. No. 93-579 (1974).
[13] *Id*.

Adherence to Privacy Act requirements is critical for a system such as the Automated Targeting System, which seeks to profile a massive amount of people, including every person "seeking to enter or exit the United States."[14] Incredibly, CBP proposes to exempt ATS 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.[15] It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to propose a secret profiling system on US citizens and be granted broad exemptions from Privacy Act obligations.

I. The Automated Targeting System's Broad Exemptions Contravene the Intent of the Privacy Act

Customs and Border Protection has invoked 5 U.S.C. §§ 552a(j)(2) and (k)(2) as authority for its exemption from specific Privacy Act requirements. These broad exemptions for law enforcement agencies and "investigatory materials collected for law enforcement purposes" would allow CBP to use this massive database with little accountability.

In its notice, CBP proposes exempting ATS 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

[14] 71 Fed. Reg. at 64544.
[15] *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).

her;[16]

- an individual may seek judicial review to enforce the statutory right of access provided by the Act,[17] 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.[18]

Companion and complementary to the right to access information is the right to correct it. Customs and Border Protection proposes exempting ATS from the Privacy Act requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;[19]

- an agency must make notes of requested amendments within the records;[20] and

- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[21]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[22]

Customs and Border Protection's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and

---

[16] 5 U.S.C. § 552a(d)(1).
[17] 5 U.S.C. § 552a(g)(1).
[18] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[19] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[20] 5 U.S.C. § 552a(d)(4).
[21] 5 U.S.C. § 552a(f)(4).
[22] H.R. Rep. No. 93-1416, at 15 (1974).

incomplete records. CBP says, "Generally, this system of records may not be accessed for purposes of determining if the system is a record pertaining to a particular individual" nor is it to be accessed "under the Privacy Act for the purpose of inspection."[23] In lieu of the statutory, judicially enforceable right of access provided by the Act, "general inquiries regarding ATS may be directed to the Customer Satisfaction Unit."[24] In its Privacy Impact Assessment for ATS, Homeland Security states, "There is no procedure to correct the risk assessment and associated rules stored in ATS."[25] (Emphasis added.) Under the redress procedure to correct data in the source systems, such as TECS, a person must write to the CBP Customer Satisfaction Unit in the Office of Field Operations.[26]

It is unknown how a person would know that there is incorrect information in ATS when the system can neither be accessed under the Privacy Act for inspection nor can it be accessed to determine if it includes an individual's record. In fact, the only indication a traveler may have that the government is keeping records about him is if he is subjected to extra scrutiny, detained or arrested at the border. This secrecy conflicts with the purposes of the Privacy Act, which was intended to provide an enforceable right of access to personal information maintained by government agencies.

Customs and Border Protection also seeks to exempt the Automated Targeting System from the fundamental Privacy Act requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary" to

---

[23] 71 Fed. Reg. at 64546.
[24] *Id*.
[25] Department of Homeland Security, Customs and Border Protection, *Privacy Impact Assessment for the Automated Targeting System* 19 (Nov. 22, 2006) [hereinafter "ATS Privacy Impact Assessment"] *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf.
[26] *Id*.

achieve a stated purpose required by Congress or the President.[27] Customs and Border Protection has not explained why it would be desirable or beneficial to maintain information in ATS that is irrelevant and unnecessary.

Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the Automated Targeting System on millions of law-abiding travelers. In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][28]

As the Office of Management and Budget noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[29] The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. The exemption from the "relevant and necessary" requirement will serve only to increase

---

[27] 5 U.S.C. § 552a(e)(1).
[28] S. Rep. No. 93-3418, at 47 (1974).
[29] Office of Management and Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28948, 28960 (July 9, 1975).

the likelihood that ATS will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing border security.

II. ATS Will Create Even More Problems than Other Deeply Flawed Traveler Profiling Schemes

According to the notice, ATS creates "risk assessments" for each person or item by "associat[ing] information obtained from CBP's cargo, travelers, and border enforcement systems with a level of risk posed by each item and person as determined through the rule based query of the cargo or personal information accessed by ATS."[30] A massive amount of information from many systems including the Treasury Enforcement Communications System, the Advance Passenger Information System, and travelers' Passenger Name Record data, which includes address and payment data, itineraries and other travelers in the same party, will be analyzed under "criteria and rules developed by CBP" that are unknown to the public.[31]

EPIC has highlighted the problems inherent in passenger profiling systems in previous testimony and comments.[32] In testimony before the National Commission on Terrorist Attacks Upon the United States (more commonly known as "the 9/11 Commission"), EPIC President Marc Rotenberg explained that "there are specific problems with information technologies for monitoring, tracking, and profiling. The

---

[30] 71 Fed. Reg. at 64544.
[31] *Id*.
[32] See EPIC's pages on Passenger Profiling, http://www.epic.org/privacy/airtravel/profiling.html; Secure Flight, http://www.epic.org/privacy/airtravel/secureflight.html; and EPIC's Spotlight on Surveillance about Registered Traveler (October 2005), http://www.epic.org/privacy/surveillance/spotlight/1005/.

techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended."[33]

The unreliability of profiling programs has been highlighted in Secure Flight, an air traveler prescreening program that was introduced a successor to the second generation Computer Assisted Passenger Prescreening System (CAPPS II), which has been abandoned.[34] Secure Flight was intended to compare passenger information from Passenger Name Records, which contain data given by passengers when they book their flights, against watch lists maintained by the federal government. However, Secure Flight morphed from a simple system of comparing names to watch lists to a complex system where profiles are created on passengers in order to assess the threat that they pose. On February 9, 2006 the head of the Transportation Security Administration told a congressional committee that Secure Flight was suspended for a comprehensive review of the program's information security measures after a Government Accountability Office ("GAO") investigation showed the program was riddled with problems.[35]

At the same hearing, the GAO revealed that TSA had approved Secure Flight to become operational in September, despite inconclusive risk assessments and 144 known

---

[33] Marc Rotenberg, President, EPIC, *Prepared Testimony and Statement for the Record of a Hearing on Security & Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003) [hereinafter "EPIC Testimony on Profiling Technologies"], *available at* http://www.epic.org/privacy/terrorism/911commtest.pdf.

[34] Department of Homeland Security, Transportation Security Administration, *Notice to establish system of records; request for comments*, 69 Fed. Reg. 57345 (Sept. 4, 2004) *available at* http://a257.g.akamaitech.net/7/257/2422/06jun20041800/edocket.access.gpo.gov/2004/04-21479.htm.

[35] Edmund S. "Kip" Hawley, Nominee for Assistant Secretary of Homeland Security, Department of Homeland Security, Transportation Security Administration, *Testimony at Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006).

security vulnerabilities. "TSA may not have proper controls in place to protect sensitive information," according to the GAO.[36] In addition to criticizing Secure Flight's lack of privacy safeguards and security vulnerabilities, the GAO also noted that the documents underlying the program "contained contradictory and missing information."[37]

These issues have led to thousands of false identifications under Secure Flight. Last year, the director of the Transportation Security Administration's redress office revealed that more than 30,000 people who are not terrorists have asked TSA to remove their names from the lists since Sept. 11, 2001.[38] The problems with Secure Flight's attempt to profile air travelers do not bode well for the attempt to profile land travelers under the Automated Targeting System. As it turns out, a GAO review of ATS has found significant problems in the program.

III. More Access and Transparency Is Needed, As the System's Accuracy and Effectiveness Are in Question

The Government Accountability Office reported earlier this year that there are significant questions about the ATS system. While it does not seem that the GAO was aware of the system's use to profile individuals, the office's review of ATS showed that CBP "currently does not have reasonable assurance that ATS is effective," testified Richard M. Stana, Director of Homeland Security and Justice Issues at the Government Accountability Office, at a Senate committee hearing in March.[39] Stana also questioned

---

[36] Cathleen Berrick, Director, Homeland Security and Justice, Government Accountability Office, *Statement at a Hearing on TSA's Secure Flight and Registered Travelers Programs Before the S. Comm. on Commerce, Science & Transportation*, 109th Cong. (Feb. 9, 2006) *available at* http://www.gao.gov/new.items/d06374t.pdf.
[37] *Id*.
[38] Anne Broache, *Tens of thousands mistakenly matched to terrorist watch lists*, CNet News.com, Dec. 6, 2005.
[39] GAO Testimony on ATS, *supra* note 8 at 5.

the accuracy and reliability of ATS risk assessments. "CBP does not yet have key internal controls in place to be reasonably certain that ATS is providing the best available information to allocate resources for targeting and inspecting containers that are the highest risk and not overlook inspecting containers that pose a threat to the nation."[40] These criticisms remained even after a 2004 GAO review suggested improvements to the system.

These accuracy and effectiveness questions are especially important as the Automated Targeting System will retain the risk assessments for 40 years, even assessments of people who are not considered a threat. "All risk assessments need to be maintained because the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified," according to Customs and Border Protection.[41] This data would be maintained in a computer database at CBP National Data Center in Washington, DC and would be available through terminals that are accessible at border points of entry and airports and seaport inspection facilities under the jurisdiction of Homeland Security.[42]

If the Automated Targeting System is exempted from these Privacy Act provisions, then the government fails to ensure the reliability of the data, provide citizens with access to their personal data, or opportunities to correct inaccurate or incomplete data. These are significant failures. The Automated Targeting System's "risk assessments" will affect every citizen who travels into or exits from the United States.

---

[40] *Id*. at 5-6.
[41] 71 Fed. Reg. at 64546.
[42] *Id*.

They will determine whether individuals will be subject to invasive searches of their persons and belongings or be permitted to cross the border.

IV. The Automated Targeting System Allows Many Federal Agencies to Improperly Access the Profiles

Customs and Border Protection has identified 15 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:

> B. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law[43]

Another category allows disclosure:

> A. To Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of civil or criminal laws.[44]

These categories are so broad as to be almost meaningless, allowing for potential disclosure to virtually any government agency worldwide for an array of actual or potential undefined violations.

Proposed routine use H. is also questionable. That provision would allow disclosure:

> H. To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.[45]

---

[43] 71 Fed. Reg. at 64545.
[44] *Id*.
[45] *Id*.

The Privacy Act [(b)(8)] already has a procedure for disclosing information pursuant to a showing of compelling circumstances. [46] The proposed Routine Use H duplicates and weakens the statutory condition of disclosure. Moreover, it does not include the disclosure notification to the individual required by the statute.[47] The agency is seeking to evade an important notification procedure required by the statute. It may not do so by its creative invocation of the routine use exception.

The agency also proposes to disclose all or a portion of the records or information contained in the system outside of the DHS when "it is suspected or confirmed that the security or confidentiality of information in the system of record has been compromised" and for other purposes. While we support notification to affected individuals in the case of security breaches, this routine use would stand the presumption of the Privacy Act on its head. Instead of the agency making known to the individual information in the possession of the agency that could have an adverse impact, it would make the information widely known across the federal government while keeping it secret from the person whose interests are supposed to be protected by the Privacy Act.

A number of the routine uses have not limited to border protection and enforcement of the customs laws. The fact that risk assessments and traveler records, including records on US citizens with an undisputed right to enter and leave the country, will be retained for up to 40 years, and disclosed to such a wide range of users, indicates that the records are not being kept and used for merely "routine" uses associated with customs and border protection but also to compile a database of the travel patterns of all

[46] 5 U.S.C. § 552a(b)(8).
[47] 5 U.S.C. § 552a(c)(3) ("Accounting of Certain Disclosures").

persons entering and leaving the US for law enforcement and intelligence purposes that have nothing to do with the protection of the US borders.

V. The Privacy Impact Assessment Only Underscores the Problems of Granting the Privacy Act Exemptions the Agency Seeks

The Privacy Impact Assessment for the Automated Targeting System, which was published three weeks after the Privacy Act notice and just a week and a half before comments were due, does nothing to ameliorate concerns about the impact of the Automated Targeting System.[48] In fact, the Privacy Impact Assessment makes clear that the program should not go forward as currently conceived. The assessment sets out the privacy risks "associated with the maintenance of the information in ATS" yet does not solve them.[49]

Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct Privacy Impact Assessments for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information.[50] The agency must conduct a Privacy Impact Assessment "before 1. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or before:

> 2. initiating a new collection of information that—
>
> 1. will be collected, maintained, or disseminated using information technology; and
>
> 2. 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.[51]

---

[48] ATS Privacy Impact Assessment, *supra* note 25.
[49] *Id*. at 8.
[50] Pub. L. No. 107-347 (2002).
[51] *Id*.

Under the Department of Homeland Security's official guidance on privacy impact assessments, the agency's Privacy Office explains that the purpose of such assessments "is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system."[52] This means that the agency should "mak[e] certain that privacy protections are built into the system from the start, not after the fact when they can be far more costly or could affect the viability of the project."[53] (emphasis added).

Yet the Department of Homeland Security did not follow either the E-Government Act of 2002 or the agency's own Privacy Impact Assessment compliance guidance. It did not conduct the Privacy Impact Assessment *before* developing or initiating the use of the Automated Targeting System to create "risk assessments" to determine whether individuals will be subject to invasive searches of their persons or belongings, and whether U.S. citizens will be permitted to enter or exit the country.

The Department of Homeland Security's official guidance explains that Privacy Impact Assessments analyze "how personal information is collected, used, stored, and protected by the Department and examines how the Department has incorporated privacy concerns throughout its development, design and deployment of the technology and/or rulemaking." But the Privacy Impact Assessment for the Automated Targeting System shows Homeland Security did not adequately incorporate privacy concerns into the

---

[52] Department of Homeland Security, Privacy Office, Privacy Impact Assessments: Official Guidance 8 (March 2006) [hereinafter "DHS Privacy Assessment Guidance"] *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_march_v5.pdf.
[53] *Id*.

system or its rulemaking. The privacy risks listed in the ATS Privacy Impact Assessment are:

> the information may not be accurate or timely because it was not collected directly from the individual, the information could be used in a manner inconsistent with the privacy policy stated at the time of collection, and/or the individual may not be aware that the information is being used by ATS for the stated purposes and/or a negative CBP action could be taken in reliance upon computer generated information in ATS that has been skewed by inaccurate data.[54]

To mitigate the risk of inaccurate or untimely data, Homeland Security says that after the system generates a risk assessment, "no action will be taken unless the information has been reviewed by a CBP officer trained in the interpretation of the information and familiar with the environment in which the information is collected and used."[55] Homeland Security also claims data review by "a well-trained CBP officer" will mitigate the risk of an "automatic negative determination."[56] However, it is unlikely that the CBP officer will undergo a thorough, thoughtful analysis of the data when importance is placed on speedily processing the more than 400 million pedestrians, passengers and privately owned vehicles that enter and exit the country annually.

In fact, Homeland Security's assessment touts the speed of the Automated Targeting system. In describing the "risk assessment" process, Homeland Security says that ATS "provides, within seconds, a risk assessment for each [private passenger] vehicle" that CPB officers use to determine "whether to allow a vehicle to cross without further inspection or to send the vehicle for secondary evaluation."[57] Under such time pressure, it would be easy for CPB officers to merely accept the computer-generated "risk

---

[54] ATS Privacy Impact Assessment, *supra* note 25 at 8.
[55] *Id*.
[56] *Id*. at 9.
[57] *Id*. at 4.

assessment," which could include inaccurate, incomplete, or untimely data seriously affecting the U.S. citizen trying to enter the country.

To mitigate the risk of violation of the privacy policy stated at the time of collection, Homeland Security's assessment says, "CBP officers are trained on the limited uses for which the information may be used in connection with their official duties." However, we have already explained that the problem is that the stated privacy policies of the systems themselves do not protect individuals' rights, so mitigation of privacy risks is impossible when the policies themselves violate individuals' privacy rights.[58]

In its official guidance on Privacy Impact Assessments, the Department of Homeland Security's Privacy Office defines the assessment as "a document that helps the public understand what information the Department is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored."[59] And Homeland Security says publication of the November 2, 2006 Federal Register Notice and Privacy Impact Assessment informs "about the specific elements of ATS" and thus mitigates individuals' lack of awareness of data being used by the Automated Targeting System.[60] We already have explained how few "specific elements" are known about the Automated Targeting System. All of the key characteristics of the system – including the assessment, the basis for the assessment, the rules that apply, and the "targeting activities" – are secret. This is not transparency. The Privacy Impact Assessment does not pierce the veil of secrecy

---

[58] *See* Section IV: The Automated Targeting System Allows Many Federal Agencies to Improperly Access the Profiles, *supra*.
[59] DHS Privacy Assessment Guidance, *supra* note 53 at 9.
[60] ATS Privacy Impact Assessment, *supra* note 25 at 8.

surrounding the Automated Targeting System and does not help the public understand the system. Though the Privacy Impact Assessment has identified substantial privacy risks in the design of the Automated Targeting System, it has failed to solve them.

While we acknowledge the effort that the agency has undertaken in preparing the Privacy Impact Assessment and examining the various issues that are required by this process, the conclusion of the analysis cannot be disputed:

- the Automated Targeting System collects personal information on US citizens from many sources, both public and private;
- makes it broadly available within the agency, across the federal government, to federal contractors, and to other governments;
- for a wide of purposes, many of which have no relationship at all to border security or other activities within the mission of the CFP;
- but lacks any meaningful rights of control, access, notice, redress, or correction to the individuals whose data is collected.

Moreover, there is insufficient information to make any meaningful representation that there is adequate security to safeguard the information or to prevent misuses.

Conclusion

For the foregoing reasons, the Automated Targeting System should not be used to establish secret profiles on individuals subject to Privacy Act safeguards. We urge the agency to suspend this activity.

If the program goes forward, CBP must revise its Privacy Act notice for the Automated Targeting System to 1) provide individuals judicially enforceable rights of access and correction; 2) limit the collection and distribution of information to only those necessary for the screening process, and 3) substantially limit the routine uses of information.

Respectfully Submitted,

ORGANIZATIONS

American Friends Service Committee
American Library Association
American Policy Center
Association of Research Libraries
Bill of Rights Defense Committee
Center for Democracy and Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Center for National Security Studies
Consumer Action
Council on American Islamic Relations
Cyber Privacy Project
Doctors for Open Government
Electronic Privacy Information Center
Ethics in Government Group
Fairfax County Privacy Council
First Amendment Foundation
Georgians for Open Government
Government Accountability Project
The Multiracial Activist
National Campaign Against Repressive Legislation
National Center for Transgender Equality
The New Grady Coalition

Privacy Rights Clearinghouse
Privacy Rights Now Coalition
The Semmelweis Society International
The Student Health Integrity Project
Unitarian Universalist Association of Congregations
U.S. Bill of Rights Foundation
World Privacy Forum

EXPERTS IN PRIVACY AND TECHNOLOGY

Prof. Ann Bartow
Prof. James Boyle
Prof. Julie E. Cohen
Philip Friedman
Deborah Hurley
Prof. Jerry Kang
Chris Larsen
Prof. Gary T. Marx
Mary Minow
Dr. Deborah Peel
Prof. Anita Ramasastry
Prof. Ronald L. Rivest
Bruce Schneier
Robert Ellis Smith
Prof. Daniel J. Solove
Prof. Frank Tuerkheimer