DEPARTMENT OF HOMELAND SECURITY

Bureau of Customs and Border Protection

Docket No. DHS6–2006–0060
Privacy Act System of Records Notice
Automated Targeting System

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

By notice published on November 2, 2006, the Department of Homeland Security, U.S. Customs and Border Protection revealed the existence of a system of records (DHS/CBP-006 -- Automated Targeting System) that will assign "risk assessments" to tens of millions of U.S. citizens who travel into or out of the United States.[1] Pursuant to the agency's notice, the Electronic Frontier Foundation ("EFF") submits these comments to address the substantial privacy issues raised by the newly disclosed system of records; to request that DHS provide greater transparency concerning the system prior to its implementation; and to urge the Department to provide an additional opportunity for public comment once additional information about the system is made public. The Department has stated that the system "will be effective December 4, 2006, unless comments are received that result in a contrary determination."[2] EFF believes that the issues raised in these comments clearly require such a "contrary determination."

The Automated Targeting System ("ATS"), as described by DHS, is a data-mining system that the agency will use to create "risk assessments" for tens of millions of travelers. It will include information that is not "relevant and necessary" to accomplish its stated purpose of improving security. Individuals will have no right to access information about themselves contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. While personal information contained in the ATS will *not* be accessible to the affected individuals, it *will* be made readily available to an untold numbers of federal, state, local and foreign agencies, as well as a wide variety of "third parties," including "contractors, grantees, experts, consultants, students, and others." The "risk assessments" created by the system and assigned to tens of millions of law-abiding individuals will be retained by the government for 40 years. Among the many details absent from its Federal Register

---

[1] Privacy Act System of Records Notice, 71 Fed. Reg. 64543 (November 2, 2006).

[2] *Id.*

notice, the agency has failed to describe the consequences that might result from a "risk assessment" score (possibly derived from inaccurate or incomplete information) indicating that an individual poses a "security threat." In short, the ATS is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.[3]

I. The ATS Lacks Adequate Transparency

In its Federal Register notice, the Department professed a desire "[t]o provide expanded notice and transparency to the public" concerning the ATS, and asserted 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."[4] In support of its suggestion that there is nothing "new" about the ATS, the Department states that the system "is the enforcement screening module associated with the Treasury Enforcement Communications System and was previously covered by the Treasury Enforcement Communications System 'System of Records Notice.'"[5]

In fact, *no* System of Records Notice for TECS has ever described (or even referenced) the ATS or any other government program that assigns "risk assessment" scores to U.S. citizens. Prior to the Department's publication of its Federal Register notice on November 2, there had been no public disclosure of the fact that the ATS was being used to assign levels of suspicion or potential risk to *individuals* – all public discussion of the system indicated that it was used to screen *cargo*. Even the Department's own Office of Inspector General, when it published its "Survey of DHS Data Mining Activities" in August 2006, reported as follows:

---

[3] 5 U.S.C. § 552a.

[4] 71 Fed. Reg. 64543

[5] *Id.*

> CBP's ACE [Automated Commercial Environment Screening and Targeting Release] is part of a long-term plan for modernizing the screening and targeting of high-risk shipments to assist agents and inspectors at our borders. It employs an expert system, the Automated Targeting System (ATS), that uses electronic shipment data to search criteria that could indicate high-risk cargo.[6]

In an effort to obtain the public release of additional information concerning the ATS and its use for purposes of assigning risk scores to individual travelers, including U.S. citizens, EFF submitted a Freedom of Information Act ("FOIA") request to the Department on November 7, 2006. EFF requested "expedited processing," citing the pending public comment period on the ATS and the need for information that would allow for an informed public debate on the significant privacy issues surrounding the system. The request sought the disclosure of, *inter alia*, any Privacy Impact Assessments ("PIA") prepared for the ATS and any records "including Privacy Act notices, which discuss or describe the use of personally-identifiable information by the CBP (or its predecessors) for purposes of screening . . . travelers."[7] To date, the Department has failed to respond to EFF's request for expedited processing and, with the exception of a PIA (discussed below), none of the requested information has been released.

Earlier this week, on November 27, DHS for the first time made available a PIA for the ATS.[8] In several respects, the PIA raises more questions than it answers. For instance, it seeks to obscure the status of citizens' access rights by asserting that applicable "[p]rocedures for individuals to gain access to data maintained in source systems that provide data used by ATS would be covered by the respective SORNs for the source systems."[9] In fact, as the Department clearly knows, most – if not all – of the "source systems" deny citizens the ability to access

---

[6] DHS Office of Inspector General, "Survey of DHS Data Mining Activities," OIG-06-56 (August 2006) at 8.

[7] Letter from David L. Sobel to Catherine M. Papoi, November 7, 2006.

[8] Privacy Impact Assessment for the Automated Targeting System, dated November 22, 2006 (although the document bears the date "November 22," the metadata contained in the PDF file indicates that it was not created until November 24; it was not posted on the DHS website until November 27).

[9] *Id.* at 18.

information about themselves.[10] Similarly, the PIA states, with respect to "procedures for correcting erroneous information," that "CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to inaccurate information."[11] The SORN for the ATS, however, unequivocally states that citizens cannot seek correction of records associated with them:

> Since this system of records may not be accessed, generally, for purposes of determining if the system contains a record pertaining to a particular individual and those records, if any, cannot be inspected, the system may not be accessed under the Privacy Act for the purpose of contesting the content of the record.[12]

As these examples illustrate, the PIA is, at best, misleading and, in important respects, clearly disingenuous. The document's deficiencies are compounded by the fact that it was not even made available for public review until several days before the agency intends to make the ATS "effective." The inadequacy of the PIA, coupled with the general lack of transparency surrounding the system, requires the Department to 1) delay implementation of the ATS; 2) make additional details concerning the system available to the public; and 3) provide further opportunity for public comment on the system.

II. The ATS Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection,

---

[10] Contrary to the agency's claimed desire to provide "expanded notice and transparency to the public," it is in fact playing "hide the ball" with respect to access and correction rights. For example, Appendix A of the ATS PIA identifies the Advance Passenger Information System ("APIS") as an "information source" for the ATS. The PIA for APIS, in turn, states that "APIS data is a subset of the system data within the Treasury Enforcement Communications System (TECS) and is covered by the System of Records Notice for TECS." 70 Fed. Reg. 17857 (April 7, 2005). The referenced SORN for TECS states that "This system of records may not be accessed under the Privacy Act for the purpose of inspection," and that "[s]ince this system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual and those records, if any, cannot be inspected, the system may not be accessed under the Privacy Act for the purpose of contesting the content of the record." 66 Fed. Reg. 52984 (October 18, 2001).

[11] *Id.* at 19.

[12] 71 Fed. Reg. 64543

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."[13] 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.[14]

The notice published by DHS exempts the ATS from nearly all of the Privacy Act's substantive and procedural rights. In support of its exemptions, the agency relies upon 5 U.S.C. §§ 552a(j)(2) & (k)(2). Each subsection raises different issues, which we address in turn.

Subsection (j)(2) provides that a system of records may be exempted from certain provisions of the Privacy Act if the system is

> maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

The ATS, as described in the agency's Federal Register notice, does not meet the criteria set forth above. With respect to the vast majority of the millions of law-abiding citizens whose names and "risk assessments" will be contained in the system, none of the three specified categories of information accurately describe the contents of the ATS. Indeed, in order for the exemption to apply, DHS would be asserting that millions of innocent citizens are "criminal offenders and alleged offenders," that those citizens are the subjects of "criminal investigation[s]," or that information concerning those citizens was "compiled at any stage of the

[13] Pub. L. No. 93-579 (1974).

[14] *Id.*

process of enforcement of the criminal laws from arrest or indictment through release from supervision." Indeed, it is clear that subsection (j)(2) does not contemplate the kind of wholesale exemption that the agency has invoked, but rather applies to individuals who are the specific subjects of criminal investigation or enforcement.

The Department's misapplication of the (j)(2) exemption is underscored by its utter failure to comply with the statutory requirement that "[a]t the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section."

Subsection (k)(2) is applicable only where the system of records is "investigatory material compiled for law enforcement purposes." The subsection further provides 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 DHS seeks to exempt the ATS from the Privacy Act's access provisions, subsection (k)(2) does not authorize the agency's action. While the Federal Register notice (despite its stated goal of transparency) does not address the potential *consequences* of the "risk assessments" that the ATS will create, it is apparent that some individuals will be denied the right to travel (and many the right to travel free of unwarranted interference) "as a result of the maintenance of such material." In a recent speech, Secretary Chertoff discussed the consequences of an individual's name being on a "list," and explained that once the agency transmits a person's name to an airline, the carrier is "actually legally obliged to deny people the opportunity to fly."[15] Under such circumstances, the Privacy Act requires the material to "be provided" to the affected individual. The full range of rights, benefits and privileges that might be denied as a result of "risk assessments" created by the ATS cannot be fully assessed until the Department explains the potential consequences of a "high risk" score. In addition, the agency has again failed to provide its "reasons" for the exemption, as the statute requires.

[15] Remarks by the Secretary of Homeland Security Michael Chertoff at the Federalist Society's Annual Lawyers Convention, November 17, 2006 (http://www.dhs.gov/xnews/speeches/sp_1163798467437.shtm)

EFF also questions whether the agency's invocation of exemptions is procedurally and substantively sound. The legislative history suggests it is not:

> Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions [of exemptible categories] then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained." The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information . . . and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.[16]

The Department's Federal Register notice is clearly not the kind of "rulemaking" that Congress envisioned. Nor has the agency stated whether, let alone why, it has determined that the application of standard Privacy Act procedures would "seriously damage" the purpose of the system of records. In addition, the application of the claimed exemptions to the *entire* system of records is clearly inappropriate, as it will obviously contain information "which should be legitimately subject to the access, challenge and disclosure provisions."[17] The agency must cure these defects before deploying the ATS.

The lack of access and correction rights is particularly troubling in light of the fact that DHS has exempted the ATS 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 achieve a stated purpose required by Congress or the President.[18] The agency does not even attempt to explain why it would be desirable or beneficial to maintain information in the ATS

---

[16] S. Rep. No. 93-3418, at 75 (1974).

[17] *See also* Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28972 (July 9, 1975) ("OMB Guidelines") ("agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted").

[18] 5 U.S.C. § 552a(e)(1).

that is irrelevant and unnecessary, although it apparently intends to do so. Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the ATS "risk assessment" process 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[.][19]

As OMB 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."[20]

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. Like the agency's other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to increase the likelihood that the ATS will become an error-filled repository of all sorts of information bearing no relationship to its stated goal of increasing security, resulting in "risk assessment" scores that will unfairly brand citizens as "suspect" for their entire lives.

Conclusion

For the foregoing reasons, EFF believes that the Department of Homeland Security must delay the scheduled December 4 effective date for the Automated Targeting System, and that

[19] S. Rep. No. 93-3418, at 47 (1974).

[20] OMB Guidelines at 28960.

the Department must provide greater transparency concerning the system prior to its implementation. We further to urge the Department to provide an additional opportunity for public comment once additional information about the system is made public.

November 30, 2006

Respectfully submitted,

David L. Sobel
Senior Counsel

Marcia Hofmann
Staff Attorney

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009
(202) 797-9009