DEPARTMENT OF HOMELAND SECURITY

Bureau of Customs and Border Protection

Docket No. DHS–2007–0043
Privacy Act of 1974: Implementation of Exemptions
Automated Targeting System

COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION

By notice of proposed rulemaking ("NPRM") published on August 6, 2007, the Department of Homeland Security, U.S. Customs and Border Protection proposes to amend its regulations to exempt the Automated Targeting System ("ATS") from most of the protections provided by the Privacy Act of 1974.[1] Pursuant to the agency's notice, the Electronic Frontier Foundation ("EFF") submits these comments to address the substantial privacy issues raised by the proposed Privacy Act exemptions; to request that DHS provide greater transparency concerning the system prior to adoption of the proposed exemptions; and to urge the Department to provide an additional opportunity for public comment once additional information about the ATS is made public.

While raising these issues, we note that the agency has revised some aspects of its initial System of Records Notice ("SORN") for the ATS published last November.[2] Several of these changes respond to concerns highlighted by EFF in its comments on the original ATS SORN, including a significant shortening of the data retention period, the clarification of access rights to Passenger Names Record ("PNR") data, and the resort to

---

[1] 72 Fed. Reg. 43567 (August 6, 2007).

[2] 71 Fed. Reg. 64543 (November 2, 2006).

formal rulemaking in order to propose Privacy Act exemptions.[3] We commend the agency for responding to earlier criticisms of the ATS, but nonetheless believe that the system continues to contravene the intent of the Privacy Act and lacks fundamental assurances of due process.

I. The ATS Continues to Lack Adequate Transparency

In its revised SORN published concurrently with the NPRM, the agency professes a desire to provide "transparency to the public about the functionality of ATS."[4] EFF shares the belief that the ATS requires greater transparency and, in an effort to obtain the public release of additional information concerning the system and its use for purposes of assigning "risk assessments" to individual travelers, submitted Freedom of Information Act ("FOIA") requests to the Department on November 7, 2006 and December 6, 2006. To date, CBP has released only a very small portion of the more than 150,000 pages of material that the agency asserts may be responsive to EFF's request. We thus believe that EFF – and the public generally – lack sufficient information to fully comment upon the system. Indeed, in seeking to justify the application of Privacy Act exemptions that will shield many of the system's details from public view, the agency asserts that greater transparency would "compromise sensitive information related to law enforcement, including matters bearing on national security," and "could present a serious impediment

---

[3] *See* Comments of the Electronic Frontier Foundation, Privacy Act System of Records Notice, Automated Targeting System (November 30, 2006) (*available at* http://www.eff.org/Privacy/ats/ats_comments.pdf).

[4] 72 Fed. Reg. 43650 (August 6, 2007).

to counterterrorism or law enforcement efforts."[5]

The continuing lack of transparency surrounding the system requires the agency to 1) delay implementation of the proposed Privacy Act exemptions; 2) make additional details concerning the system available to the public; and 3) provide further opportunity for public comment on the system.

II. The Proposed Exemptions Contravene 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, 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."[6] 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.[7]

The agency's NPRM seeks to exempt 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

---

[5] 72 Fed. Reg. 43567, 43569.

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

[7] *Id.*

> 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 August 6 notices, 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 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.[8]

[8] We are aware of the agency's response to our previous assertion that subsection (j)(2) cannot be applied to ATS records. In its discussion of public comments received in response to the November 2006 SORN, the agency states that "Exemption (j)(2) permits CBP to assert an exemption for ATS because CBP is a law enforcement agency and the information in ATS is compiled to identify suspected and known criminal offenders or alleged criminal offenders." Discussion of Public Comments Received on the Department

Subsection (k)(2) of the Privacy Act 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. 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 speech delivered late last year, 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."[9] Under such circumstances, the Privacy Act requires the material to "be provided" to the affected individual.[10]

---

of Homeland Security's Automated Targeting System Privacy Act System of Records Notice, at 17. The agency ignores the statutory language, quoted above, providing that information qualifying for exemption must "consist[] *only* of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status." (emphasis added).

[9] 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)

[10] In its discussion of public comments on the earlier SORN, the agency suggests that the subsection (k)(2) defect earlier identified by EFF is somehow cured by the recent "clarifying amendment" providing that individuals can obtain access to their PNR data. Discussion of Public Comments at 17-18. The "risk assessment analyses," however, will be exempt and not accessible to affected individuals. Since it is the maintenance of *that* material (and not PNR data) that will result in adverse determinations, we reiterate our

III. Individuals are not Provided any Meaningful Redress in the ATS

The most glaring defect in CBP's operation of the Automated Targeting System is the lack of meaningful redress provided to individuals who are adversely impacted by the system. As the Department concedes in its revised Privacy Impact Assessment for the ATS,

> The privacy risks associated with the maintenance of the information in ATS include: 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.[11]

Despite this concession that inaccurate or outdated information might result in "negative CBP action," the government continues to play a shell game with respect to redress rights, creating the illusion that such rights exist when in fact they do not.

In its NPRM, the agency unequivocally exempts the ATS from the judicially enforceable Privacy Act right to seek amendment or correction of personal information, 5 U.S.C. § 552a(d).[12] The SORN, however, suggests that redress *is* available from other agencies that maintain the information upon which the ATS risk assessments are based:

> CBP notes that ATS is a decision-support tool that compares various databases, but does not actively collect the information in those respective databases, except for PNR. When an individual is seeking redress for other

---

belief that subsection (k)(2) does not permit the blanket exemption of "risk assessment analyses."

[11] Privacy Impact Assessment for the Automated Targeting System (August 3, 2007), § 1.6.

[12] 72 Fed. Reg. 43567, 43569.

> information analyzed in ATS, such redress is properly accomplished by referring to the databases that directly collect that information.[13]

Similarly, the revised Privacy Impact Assessment for the system asserts that "ATS incorporates the procedures of the *source systems* with respect to error correction."[14]

In fact, the "source systems" provide no meaningful redress process, because they – like the ATS – are exempt from the protections of the Privacy Act. To illustrate the point, one need look no further than the Terrorist Screening Database ("TSDB"), administered by the Federal Bureau of Investigation. The TSDB is a major "source system" feeding information into the ATS.[15] Contrary to CBP's suggestion, the TSDB provides absolutely no redress process for aggrieved individuals. In a SORN for the TSDB published on August 22, 2007, the Bureau stated as follows:

> Because this system contains classified intelligence and law enforcement information related to the government's counterterrorism, law enforcement and intelligence programs, records in this system are exempt from notification, access, and amendment [under] the Privacy Act (5 U.S.C. 552a).
>
> If, however, individuals are experiencing repeated delays or difficulties during a government screening process and believe that this might be related to terrorist watch list information, they may contact the Federal agency that is conducting the screening process in question ("screening agency"). . . . By contacting the screening agency with a complaint, individuals will be able to take advantage of the procedures available to help misidentified persons and others experiencing screening problems.[16]

---

[13] 72 Fed. Reg. 43650, 43655.

[14] Privacy Impact Assessment for the Automated Targeting System (August 3, 2007), § 7.2.

[15] 72 Fed. Reg. 43650, 43653; Privacy Impact Assessment for the Automated Targeting System (August 3, 2007), §§ 1.1, 1.4, 2.3.

[16] 72 Fed. Reg. 47073, 47078 (August 22, 2007).

Here, of course, the "screening agency" – CBP – has also exempted its system from the redress provisions of the Privacy Act and asserts that "redress is properly accomplished by referring to the databases that directly collect [the contested] information." The government's handling of the redress issue is fundamentally dishonest and violates the most basic notions of due process.

Conclusion

For the foregoing reasons, EFF believes that the Department of Homeland Security must delay the implementation of its proposed Privacy Act exemptions for the Automated Targeting System, and that 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.

September 5, 2007

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