Before the

PRIVACY OFFICE
DEPARTMENT OF HOMELAND SECURITY

Washington, DC 20528

Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System	)	DHS-2007-0043 **COMMENTS OF THE IDENTITY PROJECT (IDP) AND JOHN GILMORE**

The Identity Project (IDP)

<http://www.PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

September 5, 2007

The Identity Project submits these comments in response to the Notice of Proposed Rulemaking (NPRM) published at 72 *Federal Register* 43567-43569 (August 6, 2007), docket number DHS-2007-0043, "Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System".

Under this NPRM, the Department of Homeland Security proposes to exempt from many of the requirements of the Privacy Act of 1974 much of the data in the Automated Targeting System (ATS) dossiers about individuals lifetime international (and, in many cases, domestic) travel, DHS "risk assessments", and other data contained in Passenger Name Records (PNRs) obtained by DHS from airlines, Computerized Reservation Systems (CRS's), and/or other commercial sources.

DHS proposes to exempt these records from most of the requirements of the Privacy Act, including, among others, the requirements that individuals be given access on request to records about them, that only relevant and necessary information be collected, and that when information is to be used to make decisions affecting individuals' rights, that information must be collected whenever possible directly from those individuals. DHS proposes these exemptions for **all** data about individuals in ATS records except for data in PNRs, and for much of the data in PNRs themselves.

I. ABOUT THE IDENTITY PROJECT

The Identity Project (IDP), <http://www.PapersPlease.org>, provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

II. THE ATS RECORDS SYSTEM IS PROHIBITED BY THE PRIVACY ACT OF 1974.

The first "System of Records Notice (SORN) disclosing the existence of the ATS dossiers of PNRs , "risk assessments", and other data about travelers and other individuals was published in 2006. In response to that SORN and subsequent disclosures by DHS, we filed comments pointing out, *inter alia*, that the ATS as described in the SORN is prohibited by Congressional enactments including the Privacy Act. "Comments of the Identity Project and John Gilmore, Privacy Act of 1974, System of Records Notice (SORN), DHS/CBP–2006-0060, Automated Targeting System (ATS)", December 4, 2006, available at <http://hasbrouck.org/IDP/IDP-ATS-comments.pdf>, and "Supplemental Comments of the Identity Project and John Gilmore, Privacy Act of 1974, System of Records Notice (SORN), DHS/CBP–2006-0060, Automated Targeting System (ATS)", December 29, 2006, available at <http://hasbrouck.org/IDP/IDP-ATS-comments2.pdf>.

We note that in its purported analysis of the public comments on the ATS SORN, the DHS has neither acknowledged nor responded to our comments that the ATS is prohibited by 5 U.S.C. 552a(e)(7), the section of the Privacy Act of 1974 which restricts the collection or retention of records of the exercise of rights protected by the First Amendment. "Discussion Of Public Comments Received On The Automated Targeting System System Of Records Notice Published November 2, 2006 (71 FR 64543)", <http://www.dhs.gov/xlibrary/assets/privacy/privacy_publiccmts_cbp_atsupdate.pdf>. We also note that this NPRM does not propose any exemption from this section of the Privacy Act for any ATS records. Accordingly, our comments stand as unrebutted. The ATS records system has been, is, and would remain prohibited by law, even if all of the exemptions proposed in this NPRM are finalized.

Documents released by the DHS, as a result of records requests, since the submission of our previous comments have confirmed that the ATS contains records of activities protected by the First Amendment. These are not limited to travel records (i.e. records of acts of assembly). Documents

released to John Gilmore in response to his request under the Privacy Act contained "secondary screening" which included the title of a book Mr. Gilmore was carrying when he was searched by the DHS. Mr. Gilmore's taste in literature appears to have been part of the basis for a more intrusive search of his person and belongings. Presumably, it was recorded in the ATS in order to use that record as part of the basis for future decisions by the DHS, and others to whom these records are provided, to subject Mr. Gilmore to yet more intrusive searches or other sanctions. The collection, retention, and use of such records of First Amendment protected activities violate the Privacy Act. Indeed, it is precisely to avoid such illegal misuse of records of protected activities, such as travel and expression, that the Privacy Act forbids the retention of such data without the explicit Congressional authorization that is absent here. (See 5 U.S.C. 552a (e)(7)).

Since the entire system of records is unlawful, no exemptions from it should be considered. Instead, as we pointed out in our original comments, this unlawful system of records should be shut down and the records contained in it, as well as all data obtained from it by other agencies or entities , should be destroyed.

III. THE NPRM IS FACTUALLY INACCURATE AND SELF-CONTRADICTORY.

In the current NPRM, the DHS states, “ATS-Passenger (ATS-P), one of six modules contained within ATS, maintains Passenger Name Record (PNR) data (data provided to airlines and travel agents by or on behalf of air passengers seeking to book travel).” This description of PNR data is false, and subsequent statements in the same NPRM make clear that the DHS knows that it is false. Much of the data in PNRs is not “provided to airlines and travel agents by or on behalf of air passengers seeking to book travel”.

While PNRs do contain *some* information provided by travelers or others acting on their behalf, PNRs are commercial records created and maintained by travel companies. A PNR is built using data entered by these companies, for their own purposes, or derived by them from AIRIMP (ATA/IATA Reservation Interline Message Procedure – Passenger) and other messages received by them from other travel companies. In the United States, these companies are not, in general, required to disclose any of this data to the data subjects. Travel industry standard business practice is not to disclose PNRs, or the data in them, even when disclosure is requested by data subjects.

If the only personal data in PNRs was obtained from travelers, and the ATS-P contained only PNRs, there would be no reason to exempt the ATS-P records from the requirement that data used as the basis for decisions about individuals' rights be obtained directly from those individuals. But the NPRM asserts that exemptions from the Privacy Act are needed precisely because the DHS and other recipients of this data want to rely on *other data that could not be obtained from travelers* in making decisions such as those about "permission" to travel on Federally-licensed air common carriers and passage through Federal checkpoints at airports. This contradicts the earlier claim in the NPRM that PNR data is provided by travelers and that ATS-P contains only PNRs and risk assessments.

It is evident from the claimed rationale for the proposed exemptions -- the alleged "need" for the DHS and other recipients of ATS-P data to make decisions on the basis of information that travelers themselves would not voluntarily provide, or could not provide because it originates with third parties -- that the DHS is fully aware that PNR data is not limited to data provided by or on behalf of travelers, and that the DHS is seeking to use (and perhaps is already using) this secret third-party information in PNR´s, unknown and unknowable to travelers, as part of the basis for its decision-making.

To provide the notice required by the Privacy Act, the NPRM must be corrected and reissued to accurately describe the many types and sources of non-passenger-provided third-party commercial and other data in PNRs. This is the data which, through this rulemaking, the DHS is seeking to exempt from

many of the requirements of the Privacy Act (for notice, access, accuracy, relevance, etc.), while continuing to claim the right to use in making decisions against travelers and would-be travelers.

IV. THE PROPOSED EXEMPTIONS FOR "BUSINESS CONFIDENTIAL INFORMATION" FROM THIRD PARTIES ARE INAPPROPRIATE, UNJUSTIFIED, AND CONTRARY TO THE LETTER AND INTENT OF THE PRIVACY ACT.

By this NPRM, the DHS proposes to exempt from certain requirements of the Privacy Act "business confidential information received in the PNR from the air and vessel carriers". "Business confidentiality" is not a statutory basis for exemption from the Privacy Act. Indeed, the requirements of the Privacy Act are especially essential when government agencies propose to rely on private and "confidential" commercial data, in whole or in part, in making decisions about other private parties. The special requirements of the Privacy Act for records used in making decisions about access to Federal rights, benefits, or programs apply regardless of whether the data originates with the government, the individual data subject, or – as with the proposed exemptions – with private commercial third parties.

The DHS can't have it both ways. If the so-called "business confidential" information in PNRs from airlines (and, although it is not mentioned in the SORN or the NPRM, from the many other types of travel companies from which data is received and stored in PNRs) is not used in DHS decision-making (except when it is obtained by DHS pursuant to a judicial order), then it should not be collected or retained by the DHS in the first place, and the proposed exemptions are unnecessary. On the other hand, if the DHS actually intends to use (or is already using) this third-party commercial information as the basis for decisions about Federal rights and programs such as travel by Federally-licensed air common carrier and passage through Federal checkpoints at airports, then

access to these records by the people against whom they may be used is central to both the letter and the intent of the Privacy Act.

By this NPRM, the DHS has proposed to exempt those portions of PNRs for which access and the other rights provided by the Privacy Act are most important. Individuals already know what information they provided themselves to travel companies (although they don't know, and under current U.S. law have no right to know, which of that data is entered in PNRs). What they don't know is what other information that they didn't provide has been entered in their PNRs, and which of that unknown third-party information may have been deemed "derogatory" by the DHS.

As we pointed out in detail in our previous comments, the Airline Deregulation Act of 1978 requires that airlines be Federally licensed as common carriers, and requires the DHS to consider "the public right of transit" by air when it promulgates regulations such as these proposed exemptions. As common carriers, airlines must by law transport all would-be passengers paying the fare and complying with the rules in the tariff that they have published, filed with the government, and made available for public inspection at all places where their tickets are sold. Airlines may not pick and choose which customers' business to accept, or refuse service to those they dislike.

Allowing the DHS to receive and act on information entered in PNRs by travel companies, while keeping that information secret from travelers and others, opens the door to circumvention of both the common carrier clause of the Airline Deregulation Act of 1978 and the public right of travel, through the entry of "derogatory" information in PNRs and the transmission of those PNRs to the DHS. Not only would individual airlines be able to "blacklist" disfavored individuals in this manner, for any reason and without any accountability, but the aggregation and use of this PNR data from multiple airlines would effectively turn the DHS into the compiler, maintainer, and enforcer of a joint blacklist by all airlines of anyone secretly tagged with "derogatory" information in a PNR sent to DHS by any one airline or other travel company. By denying commercially "blacklisted" individuals access to the allegedly "derogatory" third-party information about them in PNRs, and keeping its sources secret from them, the proposed exemptions would deny victims of this

blacklisting any possibility of judicial review or of recourse against those slandering or libeling them in PNRs sent to the DHS.

To make matters worse, the NPRM does not define "business confidential" information. The NPRM does not indicate who will decide what information in PNRs is business confidential", what criteria they will use in making that decision, or what procedure they will follow. The NPRM does not provide any mechanism for administrative or judicial accountability or review of such claims of "business confidentiality" or the decisions made on such claims. Each of these deficiencies is contrary to the due process requirements of the Administrative Procedure Act and the intent of the Privacy Act.

For all of these reasons, the proposed exemptions are inappropriate, unjustified, and contrary to the letter and intent of the law. Even if the ATS is not shut down entirely (as we continue to believe that it should be and, by law, must be), no PNR data in ATS records should be exempt from the Privacy Act.

V. THE PROPOSED EXEMPTIONS FROM THE REQUIRMENTS OF RELEVANCE, NECESSITY, ACCURACY, TIMELINESS, AND COMPLETENESS ARE UNJUSTIFIED.

The Privacy Act of 1974 prohibits the collection and maintenance of information by the government on its citizens unless the data is relevant and necessary to accomplish the stated purpose for its collection, and requires that the information be accurate, timely, and complete. Yet, DHS plans to retain the PNRs and other records for years after the flights. DHS here proposes to exempt the ATS from relevant and necessary limitations claiming it can "not always know in advance what information is relevant and necessary for it to complete the screening of passengers."

In advance of what? The "purpose" of ATS is to screen the names of passenger on international flights crossing US borders using list of those "known" (known to whom or through what, if any, judicial process we do not know) or suspected of being a danger to aviation safety. The screening of a passenger

is complete when the passenger's travel is concluded. Correct? If not, when is the screening process for a flight complete? Is it ever? Why would DHS wish to retain irrelevant and unnecessary records of already conducted flights? The only possible answer is that DHS intends to create a repository of travel records for future use by DHS -- to be used for purposes other than ensuring the safety of the flight at issue. This is wholly different than the stated purpose of the ATS program and the purported need for the data. Does DHS intend to use these flight records to conduct screening for future domestic flights or to screen people for reasons other than aviation safety? What else does DHS intend to use the data contained in the ATS System of records for? This NPRM does not address these important issues and is therefore deficient.

Again, "relevant" information is that which is obtained and used before the flight. After the flight it becomes irrelevant and should be discarded unless the purpose of the ATS system of records is to create permanent records to be used for purposes other than the safety and security of the flight that is the subject of the records. The NPRM does not address this issue and is therefore deficient.

The term "suspected terrorist" is troublesome. Does the term "suspected terrorist" mean those on a "watch list" as opposed to those on a "no-fly list"? Or does it mean everyone who wants to fly? DHS states in this NPRM that "information relating to known or suspected terrorists is not always collected in a manner that permits immediate verification or determination of relevancy to a DHS purpose." DHS also states that "DHS and other agencies may not always know what information about an encounter with a known or suspected terrorist will be relevant to law enforcement for the purpose of conducting an operational response." For these reasons DHS asks to be exempt from the requirement that the data be relevant, necessary, accurate, timely, and complete. Is everybody that flies a "suspected terrorist" in the eyes of DHS? Does "suspected terrorist" mean everybody other than a "known" terrorist? If so, this NPRM is deficient because it is misleading and should for clarity and honesty use the term "everyone" or "everyone other than known terrorists" instead of "suspected terrorists."

VI. CONCLUSION AND RECOMMENDATIONS

The NPRM should be withdrawn. The ATS records system should be shut down, and all records contained in it as well as all data obtained from it by other agencies or entities should be destroyed.

Respectfully submitted,

.

The Identity Project (IDP)

<http://www.PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

_____/s/_____

Edward Hasbrouck,

Consultant to IDP on travel-related issues

James P. Harrison

Staff Attorney, First Amendment Project

Director, IDP

John Gilmore

Post Office Box 170608

San Francisco, CA 94117