THE PRACTICAL NOMAD

EDWARD HASBROUCK
1130 Treat Avenue, San Francisco, CA 94110, USA
phone +1-415-824-0214
edward@hasbrouck.org
http://hasbrouck.org

The Practical Nomad Guide to the Online Travel Marketplace (2001)
The Practical Nomad: How to Travel Around the World (2nd edition, 2000)
http://www.practicalnomad.com

23 February 2003

Documentary Services Division
Attention: Docket Section, Room PL-401
Docket No. OST-1996-1437
U.S. Department of Transportation, SVC-124
Washington, DC 20590, USA

CONSOLIDATED COMMENTS OF EDWARD HASBROUCK RE: ESTABLISHMENT AND EXEMPTION FROM THE PRIVACY ACT OF RECORDS SYSTEM DOT/TSA 010, "AVIATION SECURITY-SCREENING RECORDS (ASSR)"

**(1) "Notice To Amend A System Of Records",
Docket No. OST-1996-1437-11, 68 *Federal Register* 2101-2103,
<http://dms.dot.gov/search/document.cfm?documentid=233481&docketid=1437>**

**(2) "Notice Of Proposed Rulemaking",
Docket No. OST-1996-1437-9, 68 *Federal Register* 2002,
<http://dms.dot.gov/search/document.cfm?documentid=212050&docketid=1437>**

ABSTRACT:
=========

The Department has not satisfied the statutory notice and comment requirements; the proposals exceed the Department's statutory authority; the Department has failed to consider factors required by statute to be considered; the Department has failed to conduct the required analysis of regulatory impacts; and the proposed system of records and its uses would be unconstitutional.

The Department should withdraw the proposals to create this system of records and to exempt it from the Privacy Act. If they are not withdrawn, the Department should extend the time for filing of comments until at least 17 March 2003, and allow at least 30 days after the department publishes the final proposals, and notifies Congress that it has done so, before their effective date. The Department should more fully disclose the purposes and intended uses of the system of records, and consider whether it is necessary for those purposes, its economic impacts (particularly in light of the contractual privacy commitments of airlines, CRS's/GDS's, airline data hosting systems, and travel agencies), and the impact of the proposals on the public interest in air transportation (particularly if airlines, CRS's/GDS's, and travel agencies are obligated to cease operations to countries, and to refuse to do business with persons and entities subject to the jurisdiction of countries, with whose privacy regulations the proposals are incompatible).

At most, the system of records and the information transferred to the Department should be limited to "passenger lists", which have only a single data field -- "passenger name" -- for each passenger, and do not include any of the additional data fields contained in passenger manifests, PNR's, "associated data", etc. Any recipient of data should be required to purge such data whenever the data in the original system is purged. If the proposed system of records is to be used in restricting travel, mechanisms for due process should be included in the proposal.

COMMENTS:
=========

I am a travel expert and consultant, consumer advocate for travellers, author of two books of consumer advice for travellers on issues including privacy and travel data, author and maintainer since 1991 of the Usenet FAQ on international airfares, author/publisher of a Web site of consumer advice and information for travellers, staff employee of an Internet travel agency specializing exclusively in international air travel, and the leading privacy advocate in the USA on travel issues.

These comments are submitted strictly on my own behalf, and as an independent consumer and privacy advocate for travellers. They do not necessarily represent the opinions or beliefs of my publisher, my employers, or any of my consulting clients.

1. THE DEPARTMENT HAS NOT SATISFIED THE STATUTORY NOTICE AND COMMENT REQUIREMENTS FOR SUCH A REGULATION.

Under the Department's regulations and the provisions of both the Privacy Act and the Aviation and Transportation Security Act, these proposals require prior public notice and opportunity for comment. That notice and opportunity for comment have not yet been provided; the notices of these proposals are both procedurally and substantively deficient.

The "Notice To Amend A System Of Records" was published in the *Federal Register* on 15 January 2003. The print publication contained no docket number or RIN number and no address for comments, and did not appear in any form whatsoever in the Department's online Docket Management System. Six weeks later, 21 February 2003, on the last business day before the scheduled effective date of the proposal, in response to my repeated e-mail messages to the department's designated contact for this proposal, it was filed in the Docket Management System and assigned Docket No. OST-1996-1437-11.

It is still impossible for commenters to determine the correct RIN number applicable to these notices. In the *Federal Register*, the "Notice of Proposed Rulemaking" (68 *F.R.* 2002) was identified as RIN 2105-AD23; no RIN number(and no docket number) was included in the "Notice to Amend a System of Records". In the Department's Docket Management System at <http://dms.dot.gov/reports/fr.htm> and <http://dms.dot.gov/search/searchResultsSimple.cfm?numberValue=1437&searchType=docket>, both these docket items are identified with a different RIN number, RIN 2105-AC57.

The failure to include a docket number, RIN number, or address for comments in the *Federal Register* publication of the "Notice To Amend A System Of Records", and the absence of that notice from the DOT Docket Management System (in which regulatory filings are required to be filed electronically, with equal validity with hardcopy filings), renders the print publication insufficient as public notice.

The DOT Docket Management System correctly indicates the effective filing date of the "Notice To Amend A System Of Records", Docket No. OST-1996-1437-11, as 21 February 2003. This is the date it was assigned a docket number, published electronically, and opened for electronic comments.

It could reasonably be expected that those individuals, organizations, and entities most interested in, and desirous of commenting on, proposals concerning electronic databases would be most likely to rely on the electronic docket for notice of such proposals, and to wish to file their comments electronically.

Not surprisingly, in the six weeks from the publication of the printed *Federal Register* notice on 15 January 2003 (which contained no address for comments) until the electronic filing of the notice on 21 February 2003, no comments were received on what has now been assigned Docket No. OST-1996-1437-11, and only two comments on Docket No. OST-1996-1437-9 (which pertains to the exemption from the Privacy Act of the system of records described in the then undocketed "Notice To Amend A System Of Records").

The day that the notice was assigned a docket number and filed electronically (the only business day before the scheduled effective date of the proposal), 39 electronic comments were received. It's clear that the procedural deficiencies in the notice -- the absence of a docket number or comment address in the print notice, and the delay in electronic filing and assignment of a docket number -- have deprived interested parties of notice and opportunity to comment, and that the comment period should be extended.

To the extent that the proposals rely on 49 U.S.C. 44901 for authorization, they are subject to subsection (h)(2) of that section, which provides that the Under Secretary "shall advise Congress of a regulation to be prescribed under this section at least 30 days before the effective date of the regulation, unless the Under Secretary decides an emergency exists requiring the regulation to become effective in fewer than 30 days and notifies Congress of that decision."

The proposals contain no evidence that the requisite notice has been provided to Congress. Assuming, *arguendo*, that the filing of the "Notice to Amend A System Of Records" on 21 February 2003 constitutes in and of itself the requisite notice to Congress, the effective date of the proposal must be postponed until no earlier than 30 days after the date of that notice, 17 March 2003. If any changes are made to the proposals, they must be republished, with an effective date no less than 30 days after their publication in final form and notification to Congress.

The proposals should also be revised clearly to limit their effect to data collected after the statutorily required notice period. There is no way to remove most information from airline PNR's (each cancelled item is moved to the "history" section of the PNR, but remains accessible to airline and travel agency personnel alike), or to delete or purge a PNR. Thus the only way to avoid having PNR's incorporated into the ASSR system that contain information that individuals provided under the belief that the information would not be provided to the government, and would not consent to provide once notice was given of its intended use, would be to limit the proposals to PNR's with a creation date after the effective date of the final rule, regardless of the date of travel. The proposals should therefore be revised to clearly limit their effect to PNR's created after their effective date, regardless of the date of travel.

The proposals also suffer from substantive notice deficiencies.

The description of the categories of records in the ASSR system is insufficient to enable a reasonable person to determine which information they might provide, or which others might provide, would be entered into this system, or to make informed decisions as to whether to provide information that might be so used.

The description of the categories of records in the ASSR system is also insufficient to enable travel intermediaries, such as travel agents, travel agencies, CRS's/GDS's, and airline hosting systems to know which information they enter or disclose about travellers will be disclosed to whom by the recipients(s), or to advise their clients and customers how their information might be used (as they are required to do, in many cases, under their existing privacy policies and contractual commitments to their clients and customers, and under other countries' laws).

And the description of the categories of records in the ASSR system is insufficient to permit a determination as to whether or not the data to be collected would be relevant, useful, or necessary to any statutory purpose.

The description of the categories of individuals covered by the system is manifestly incomplete, given the categories of records, particularly Passenger Name Records (PNR's), proposed to be included. PNR's contain detailed, personally identifiable data on several categories of individuals not mentioned in the notice.

In addition to travellers, PNR's contain data on individuals who made reservations, but did not actually travel -- even if they never even purchased tickets. To the best of my knowledge, no CRS/GDS or airline hosting system includes a mechanism for deleting or purging PNR's pertaining to cancelled or unticketed reservations. A PNR can be cancelled, but the audit trail or "history" of the PNR, showing when and by whom each entry in the PNR was made, is always retained at least until the last date of any of the reservations, active or cancelled, in the PNR.

PNR's also contain data on individuals who never travel by air at all: the vast majority of car rental and hotel reservations, and some bookings for cruises and other travel services, made through travel agencies, are made through a CRS/GDS and entered into a PNR, even if they do not involve air travel. Because of the use of PNR's in a CRS/GDS as a CRM system and the basis of most travel agency accounting systems, most corporate and many leisure travel agencies create PNR's for all reservations of any type, whether or not they were actually booked through a CRS/GDS.

Each entry in a PNR "history" includes a "received from" field identifying the person who requested the reservation or change. PNR's thus include personally identifiable information on travel arrangers, such as corporate and professional personal assistants and administrative staff, travel managers, event organizers, and family members and friends assisting with travel arrangements.

PNR's also include extremely detailed, personally identifiable data on travel industry personnel, particularly travel agents and airline reservation, check-in, and ticketing staff. Each entry in a PNR history includes a field identifying the unique "agent sine" or log-in ID of the person making the entry, along with the city or "pseudo-city" (airline office or travel agency branch or location) and the LNIATA or "set address" of the terminal or data connection on which the entry was made (the CRS/GDS or airline hosting system counterpart of an Internet IP address) and the exact time of the entry. In the aggregate, PNR's thus provide a comprehensive and extremely detailed record of every entry made by tens of thousands of travel agents and airline reservation staff: what was entered, when, where, by whom, and for whom.

In some cases, billing codes entered in PNR's contain personal information on the clients of travellers -- including information protected by attorney-client, journalistic, and other privileges. Corporate travel agencies routinely include codes in PNR's to

indicate to the traveller (or the traveller's employer), to which department, project, or client the cost of the trip is to be billed. In the case of a law firm, these entries routinely identify the specific client, case, or matter on whose behalf or at whose expense the travel was undertaken. Thus clients of law firms, consultants, financial advisors, and other professionals could find themselves identifiably the subject of data in PNR's, and thus of data in the proposed ASSR system.

The proposal should be republished with a more detailed description of the specific data fields proposed to be included in the ASSR system, and with a complete list of the categories of individuals about whom personal data would be included. Only then could there be full consideration of the economic, international, contractual, or privacy impact of the proposal.

2. THE PROPOSED SYSTEM OF RECORDS EXCEEDS THE DEPARTMENT'S STATUTORY AUTHORITY.

The "Notice to Amend a System of Records" cites as "authority for maintenance of the system" 49 U.S.C. 114, 44901, and 44903. These three statutory sections are discussed in turn below. Only a small portion of the proposal is even arguably authorized by any of these statutory sections, all of which were enacted as part of the Aviation and Transportation Security Act of 2001, P.L. 107-71, 115 Stat. 597 *et seq*.

In general, the intent of Congress in enacting the Aviation and Transportation Security Act should be interpreted in light of its action earlier this month to forbid the Defense Advanced Research Projects Agency from developing or deploying DARPA's proposed "Total Information Awareness" (TIA) program. Presumably, Congress would not have voted to forbid DARPA to proceed with TIA, because of its impact on personal privacy, if Congress believed that it had already authorized a program with the same impact under the Aviation and Transportation Security Act.

This proposal would involve the collection and integration of almost exactly the same sources and categories of data which were proposed to be included in the TIA program. As in the proposed TIA program, the ASSR system would, it appears, operate through correlation, pattern recognition, profiling, and "threat assessment", based on these multiple sources of data and what they reveal, in combination, about individuals. Like the TIA program, the proposal for the ASSR system would permit data to be

“shared” with (i.e disclosed to), and then retained indefinitely by, any agency in the Intelligence Community.

The only difference between the TIA program and the Department’s current proposals is that the ASSR system would, at least nominally, be limited to those who travel at some time by air. Given the prevalence of air travel in the USA, that is not a very significant limitation or distinction.

Were the Department to proceed with these proposals without modification, it would effectively constitute the implementation of the “Total Information Awareness” program -- under another name and by a different department, but still in contravention of the clear intent of Congress that TIA not be implemented.

(A) 49 U.S.C. 114

The only arguably relevant portion of section 114 is subsection (h), "Management of Security Information".

49 U.S.C. 114, subsection (h)(1) requires the Under Secretary to "enter into memoranda of understanding with Federal agencies or other entities to share or otherwise cross-check as necessary data on individuals identified on Federal agency databases who may pose a risk to transportation or national security."

The authority conveyed by this subsection is limited to the authority to enter into memoranda of understanding, not to issue mandatory regulations or compel disclosure of information.

Because much of the data concerning passengers held by airlines, CRS's/GDS's, airline data hosting systems, and travel agencies is received under confidentiality agreements which restrict its disclosure, the wide range of data contemplated in the proposed ASSR System could not be provided under voluntary memoranda of understanding by those entities, but could be provided, if at all, only under government compulsion. Sub-section (h)(1) authorizes no such compulsion to breach privacy contracts.

Any data sharing under subsection (h)(1) must be "necessary". Necessity is a high statutory standard: the department would need to show not just that an action under this sub-section is reasonably related to a statutory purpose, or would actually advance that interest, but that no less intrusive and/or less burdensome alternative action could satisfy the government's

interests. No showing or even claim has yet been made that the breadth of information proposed to be collected and exempted form the Privacy Act under the ASSR system would even be related to, much less essential for, any permissible or authorized government interest. There is no evidence that the department has considered less intrusive and burdensome alternatives, despite the substantial body of expert opinion and evidence -- and testimony before the Department in past proceedings -- that profiling systems to select passengers for screening are less effective, as well as more intrusive and burdensome, than universal screening of all passengers in the same manner.

Subsection (h)(1) applies only to "individuals identified on Federal agency databases" as potential threats. But the proposed ASSR system would include two distinct components, only one of which would pertain to people already identified as potential threats. The other portion of the ASSR proposal, for collection of data on all "Individuals traveling to, from, or within the United States (U.S.) by passenger air transportation", is wholly unauthorized by any conceivable interpretation of subsection (h)(1), and this portion of the proposal should be withdrawn.

Subsection (h)(2) requires the Department to "establish procedures for notifying the Administrator of the Federal Aviation Administration, appropriate State and local law enforcement officials, and airport or airline security officers of the identity of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety". The only information authorized to be disclosed under this subsection is the "identity" of an individual already identified as a threat, and only to specified types of entities. But disclosure of information to other entities under the proposed ASSR is not limited to those categories of entities, is not limited to identity data, and is not limited to those who have already been identified as threats.

Subsection (h)(3) authorizes the Department to, "in consultation with other appropriate Federal agencies and air carriers, establish policies and procedures requiring air carriers- (A) to use information from government agencies to identify individuals on passenger lists who may be a threat to civil aviation or national security; and (B) if such an individual is identified, notify appropriate law enforcement agencies, prevent the individual from boarding an aircraft, or take other appropriate action with respect to that individual."

Assuming, *arguendo*, that the department has conducted the mandated consultation with the air carriers (of which there is no evidence in the proposal) and that clause (B) is constitutional (which would require at a minimum due process provisions for the imposition of restrictions on travel, of which there are none in the proposal), subsection (h)(3) is, like subsection (h)(2), limited to information used to identify individuals. Most of the information proposed to be included in the ASSR system has no conceivable utility in identifying individuals, but is merely information about individuals and their activities.

Finally, subsection (h)(4) requires the Department to "consider requiring passenger air carriers to share passenger lists with appropriate Federal agencies for the purpose of identifying individuals who may pose a threat to aviation safety or national security." Presumably, this rulemaking proceeding is that consideration. But this subsection is limited to sharing of data between airlines and Federal agencies, whereas the proposals provide for sharing of this information between a much wider range of entities.

This subsection is the only provision of any of the statutes cited as authority for the proposal that authorizes the department to compel airlines (or any other private or non-governmental entities) to provide data to the government.

But this statutory power of compulsion is explicitly limited to the provision by airlines of "passenger lists". A "passenger list", in common language and in the specialized usage of the airline industry, is a list of passengers. It contains a single data field, "passenger name", for each passenger.

The Aviation and Transportation Security Act clearly distinguishes a "passenger list" from a "passenger manifest", which contains a limited number of additional data items for each passengers's contact and travel document information (see 49 U.S.C. 44909). A close reading of the sections of the Aviation and Transportation Security Act using the terms "passenger list" and “passenger manifest" makes apparent that they are not used interchangeably, and that "passenger list" is a narrower term than "passenger manifest".

CRS's/GDS's, airline hosting companies, and travel agencies are under no statutory compulsion to provide any passenger data to the Department. Airlines can be required, at most, to provide

lists of passengers names, and no other passenger data. All entities other than airlines, and airlines with respect to all information except passenger lists, remain bound by their contractual commitments to their customers not to divulge information provided under promise of confidentiality.

Yet the proposed ASSR system is not limited to passenger lists, or even to passenger manifests, and is not limited to information provided by airlines. The ASSR system would include "Passenger Name Records (PNRs) and associated data; reservation and manifest information of passenger carriers and, in the case of individuals who are deemed to pose a possible risk to transportation security, record categories may include: risk assessment reports; financial and transactional data; public source information; proprietary data; and information from law enforcement and intelligence sources."

At the absolute minimum, the proposals must, under the cited statutes, be revised to limit any compelled provision of information to the provision of passenger names by airlines, excluding the provision of data by other entities or the provision by airlines of any data other than passenger names.

(B) 49 U.S.C. 44901

The only portion of 49 U.S.C. 44901 that would conceivably provide authorization for any portion of the ASSR proposals is the passing reference in subsection (a), as an exception, to "screening under the CAPPS" (Computer-Assisted Passenger Prescreening System) program. But neither the "Notice To Amend A System Of Records" nor the "Notice Of Proposed Rulemaking" makes any mention of CAPPS. To the extent that the ASSR system is not to be used in conjunction with CAPPS, there is nothing in section 44901 to authorize it. To the extent that it is intended to be used in conjunction with CAPPS, the notice provided by the proposals, particularly the statement of the "Uses of the records maintained in the system", is deficient, and should be revised and republished, followed by a new comment period.

CAPPS is an intensely controversial system. Whether it would be effective, justified, and /or preferable to alternatives is a matter of considerable dispute. If the proposals had stated that data maintained in the ASSR system would be used in conjunction with CAPPS, the Department would undoubtedly have received a much greater volume of comments from interested and concerned parties.

(C) 49 U.S.C. 44903

The only arguably relevant subsection of 49 U.S.C. 44903 is subsection (b), which provides that, "The Under Secretary shall prescribe regulations to protect passengers and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence or aircraft piracy."

The only way that proposals for data collection and sharing -- especially data related to passengers who are not considered to pose any threat, and data so distantly related, if at all, to "criminal violence or aircraft piracy" -- could conceivably be authorized under this subsection would be through use of this data in CAPPS. But, as noted above, the proposals do not include CAPPS in the intended uses of the system of records.

Accordingly, the proposals should either be withdrawn -- at least to the extent that they are claimed to be authorized under section 44903 -- or republished with a disclosure of their intended use in conjunction with CAPPS, and an opportunity for comment on whether such use would, in fact, "protect passengers and property on ... aircraft ... against... criminal violence or aircraft piracy", which I do not believe they would do.

(D) The Privacy Act of 1974

The “Notice To Amend A System Of records” provides for information to be transferred to an extraordinarily wide range of domestic and foreign entities, including to any “agencies of the Intelligence Community” and to any “foreign government authorities in accordance with ... informal ... agreements”.

There is no provision for protection of information against unauthorized disclosure, once thus transferred. And there is no provision for deletion or purging of such information. In accordance with the Privacy Act of 1974, the proposal should be revised to require that any transfer of data to an entity outside the Department, and particularly to any entity outside the government of the USA, should be subject to an enforceable commitment by the recipient of the data that it will not be further transferred, disclosed, or “shared”, and that it will be purged by the recipient when the original data is purged by the Department. And the proposal should be revised to require the

Department to notify any other recipients of data from the system whenever the Department purges that data.

3. THE DEPARTMENT HAS FAILED TO CONSIDER FACTORS REQUIRED BY STATUTE TO BE CONSIDERED IN PRESCRIBING SUCH A REGULATION.

49 U.S.C. 44903, cited in the "Notice To Amend A System Of Records" as its authority, requires in subsection (b) that the Department consider a list of specific factors when prescribing regulations under that section. There is no evidence that those factors have been considered by the Department. If they were to be considered, they would strongly contra-indicate the proposals.

Subsection (b)(2)(A) requires the Department to "consider whether a proposed regulation is consistent with protecting passengers". One of things against which passengers need to be, and should be, protected, is invasion of privacy.

Subsection (b)(3)(A) requires that the Department, "to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure their safety." One of the ways that passengers' safety can be endangered is through breach of privacy.

Insufficient safeguards for disclosure of PNR information already pose a grave danger of privacy invasion and abuse, potentially contributing to or facilitating stalking of travellers, burglary of homes determined from travel data to be vacant, and other safety hazards, in addition to the privacy invasion itself. (See my discussion at <http://hasbrouck.org/articles/watching.html>.) The more data is collected and cross-referenced, and the more widely such information is "shared" and disseminated, the greater the risk posed to passengers and their safety and security through breach of privacy and its consequences.

For example, I have had as clients, in my work as a travel agent, international human rights attorneys whose safety was gravely jeopardized, and whose ability to protect the safety of their clients was severely impaired, by the unauthorized disclosure of information from their PNR's (by, so far as I could tell, either the staff of a USA-based airline or a travel agent appointed by that airline) to a foreign government entity.

Data collection, sharing, and disclosure, especially compulsory or secret data collection or disclosure, should be recognized by

the Department under 49 U.S.C 44903, subsections (b)(2)(A) and (b)(3)(A), as being inconsistent with protecting passengers against privacy invasion and other abuse, and as jeopardizing their safety. Proposals under this statute can be justified only after consideration of these negative effects of data collection and dissemination, and only on a showing of likely benefits sufficient to outweigh these risks to passenger safety.

As quoted above, subsection (b)(3) requires that the Department prescribe, "to the maximum extent practicable, a uniform procedure for searching and detaining passengers."

CAPPS by definition exists to facilitate non-uniformity in searching: it is a system for differentiation of searching. As such, it can be prescribed by Department regulation under this section only after consideration and a finding by the Department that no uniform procedure is practicable. There is no evidence in the proposal that the Department has even considered the practicability of alternatives to CAPPS, much less that all such alternatives have been found impracticable.

In similar vein, subsection (b)(4) requires the Department to "consider the extent to which a proposed regulation will carry out this section." There is no evidence that these proposals or CAPPS, if it included the full range of data contemplated by these proposals, would be practicable or effective in serving any permissible statutory purpose, or that the Department has considered whether they would do so.

Finally, subsection (b)(2)(B) requires that the Department "consider whether a proposed regulation is consistent with ... the public interest in promoting air transportation and intrastate air transportation".

As discussed more fully below, the proposed ASSR system, especially if it is exempted from the Privacy Act, would create obligations for airlines, CRS's/GDS's, airline hosting systems, and travel agencies and agents incompatible with their obligations to persons subject to the jurisdiction of the Canadian Personal Information Protection and Electronic Documents Act and the European Union Data Privacy Directive, and their contractual commitments to abide by those Canadian and EU laws.

If it proves impossible for the travel industry to comply with both these proposals and the relevant Canadian and EU privacy

laws, the result would be that flights could not legally be operated between the USA and Canada and/or the USA and the EU.

This would clearly be a consequence inconsistent with the public interest in promoting air transportation. As such, it must, under this statute, be considered by the Department. Accordingly, these proposals should be withdrawn until the Department has considered whether they can be complied with consistently with compliance with Canadian and EU privacy law.

Presumably, that consideration could only effectively be conducted with the participation of representatives of the Office of the Privacy Commissioner of Canada and the European Union Data Privacy Commission, in addition to experts on international privacy law familiar with the privacy laws of other countries that might raise similar compatibility and compliance issues.

For all these reasons the proposals should be withdrawn until the Department has considered and stated its findings with respect to these concerns mandated by statute to be considered.

4. THE DEPARTMENT HAS FAILED TO CONDUCT THE REQUIRED ANALYSIS OF REGULATORY IMPACTS.

According to the "Analysis of Regulatory Impacts" in the "Notice Of Proposed Rulemaking", "This proposal is not a 'significant regulatory action' within the meaning of Executive Order 12886. It is also not significant within the definition in DOT's Regulatory Policies and Procedures, 49 FR 11034 (1979), in part because it does not involve any change in important Departmental policies. Because the economic impact should be minimal, further regulatory evaluation is not necessary. Moreover, I certify that this proposal would not have a significant economic impact on a substantial number of small entities, because the reporting requirements, themselves, are not changed and because it applies only to information on individuals."

This analysis, and this certification, are entirely unsupportable. Real-time access by the Department to all airline PNR's, as appears to be contemplated by the proposal (although, as noted, its vagueness precludes our knowing for certain), and the compilation and correlation of airline data with "associated", private, commercial, financial, and "public source" data, would be a dramatic change in important Departmental policies.

Tens of millions of airline PNR's, involving a significant fraction of the citizens and residents of the USA as well as vast numbers of current and prospective foreign residents and visitors, are active at any given time. The proposed ASSR system would almost certainly contain data on more individuals and entities than any other system of records exempt from the Privacy Act. The retention of any or all of these "associated" and other records on an unknown (and, if exempted from the Privacy Act, unknowable) portion of those individuals for up to 50 years would result in one of the largest, and most intimately revealing, government databases about individuals and their movements, activities, interests, associations, and behaviors.

Travel data is the largest, most sensitive, and most significant category of personal information not yet subject, in the USA, to any sector-specific Federal privacy regulations (such as apply to legal, financial, and medical information). This is in marked contrast to other countries, most of which have recognized the significance of travel data by putting it in the forefront of their privacy-protection systems. Canada, for example, included airlines (and, to the extent they function as agents of the airlines, travel agencies) in the first phase of its ongoing implementation of its Personal Information Protection and Electronic Documents Act -- three years earlier than entities in most other sectors deemed less critical to personal privacy were required to have complied with that Act.

PNR’s don’t just contain flight reservations and ticket records. They include car, hotel, cruise, tour, sightseeing, and theater ticket bookings, among other types of entries.

PNR’s show where you went who went, when, with whom, for how long, and at whose expense. Behind the closed doors of your hotel room, with a particular other person, they show whether you asked for one bed or two. Through departmental and project billing codes, they reveal confidential internal corporate and other organization structures and lines of authority and show which people were involved in work together, even if they travelled separately. Particularly in the aggregate, they reveal trade secrets, insider financial information, and information protected by attorney-client, journalistic, and other privileges.

Through meeting codes used for convention and other discounts, PNR’s reveal affiliations -- even with organizations whose membership lists are closely-held secrets not required to be

divulged to the government. Through special service codes, they reveal details of travellers' physical and medical conditions. (There is no evidence that the Department has evaluated these proposals for compliance with the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), despite the fact that PNR's clearly contain data subject to HIPAA.) Through special meal requests, they contain indications of travellers' religious practices -- a category of information specially protected by many countries.

Compilation of all this personal data by the government cannot accurately be described as "not a significant regulatory action".

The economic impact of the proposals would not be minimal, the proposals would have a significant economic impact on a substantial number of small entities, and the proposals apply to vast amounts of detailed information on businesses and corporations as well as individuals.

The economic impact of the proposals would be immense. If the ASSR system were not exempted from the Privacy Act, and if airlines, CRS's/GDS's, airline hosting systems, and travel agencies could comply without violating the EU Data Directive or the Canadian Personal Information Protection and Electronic Documents Act (all of which seem extremely unlikely to be possible), compliance would cost the travel industry at least hundreds of millions of dollars, probably billions, and take many months to implement.

If the ASSR system were exempted from the Privacy Act, it is almost inconceivable that airlines or other entities could comply with both the requirements imposed by this proposal and the pre-existing privacy laws and regulations of other countries, especially those of the European Union and Canada. Airlines, CRS's/GDS's, airline hosting systems, and travel agencies would thus be forced to choose between (1) operating and accepting business from customers in Canada and/or the EU, but not operating or accepting business from the USA, (2) operating and accepting business from customers in the USA, but not operating or accepting business from those in (or subject to the jurisdiction of) Canada or the EU, or (3) risking regulatory enforcement action and sanctions for noncompliance with the ASSR regulations, the EU Data Privacy Directive, and/or the Canadian Personal Information Protection and Electronic Documents Act.

Choices (1) or (2) would result in cessation of transborder air service between the USA and Canada and/or trans-Atlantic and polar air service between the USA and the EU, with disastrous direct consequences for the travel and transportation industries and international trade, and secondary impacts on all sectors of the economy. Costs would be measured at least in tens of billions of dollars for even a short interruption of air services, much more for a prolonged or permanent one.

Choice (3) would likely precipitate serious diplomatic rifts with the EU and/or Canada, with substantial likelihood of enforcement action against air carriers and other entities, and the potential for other trade sanctions against the USA for failure to respect the privacy rights of other countries' citizens and residents. Government-imposed penalties and damage awards for breach of Canadian and/or EU citizens' privacy rights could easily bankrupt USA-based airlines and CRS's/GDS's, disrupting air transport and trade. In this scenario as well, costs could be measured at least in the tens of billions of dollars.

Even if immediate enforcement action by Canadian or EU authorities were not forthcoming, the possibility that it could be brought at any time would greatly increase the risk of investment in airlines or other travel companies, potentially limiting their access to critically-needed investment capital and sabotaging any chance of recovery for many distressed airlines and other travel companies.

The costs of compliance with these proposals would be a severe, perhaps catastrophic, burden for the tens of thousands of travel agencies in the USA, most of which are small businesses with only a handful of employees.

Current standard industry practice for travel agencies is to treat their "pseudo-city" in a CRS/GDS as their primary repository of customer and transaction data. CRS's/GDS's encourage this, and have developed an extensive range of reporting, quality control, MIS, CRM, etc. systems and services for travel agencies that depend on the storage of large amounts of agency and agency client data -- much of it not strictly essential to air reservations and ticketing-- in the CRS/GDS. The majority of travel agencies have no electronic customer database, and many have no transaction records, other than those they maintain in a CRS/GDS.

CRS's/GDS's support this practice (which helps promote loyalty by their agency customers), and encourage the storage of even inessential data in the CRS/GDS by committing themselves contractually not to disclose information entered in the CRS/GDS by travel agencies, except with the consent of the travel agency or when required to do so by government order.

Travel agencies' customers, in turn, routinely include non-disclosure agreements (NDA's) in their contracts for travel agency services. These NDA's are critical to many businesses, since travel agents of necessity are privy to large amount of confidential information regarding business organizational structures and activities; customer and supplier contacts; negotiations for potential mergers, acquisitions, and partnerships; and confidential personnel information. For professionals such as lawyers and doctors, whose travel records include privileged information concerning their client relationships, a confidentiality contract is an essential legal prerequisite to doing business with a travel agent.

If the proposals are adopted, travel agents will no longer be able to rely on a CRS/GDS to respect the privacy of information entered into a PNR, since the CRS/GDS or airline might be forced to disclose that information to the Department for use in the ASSR system.

Accordingly, travel agents will each be obliged -- in order to honor their contractual privacy commitments to their clients -- to construct independent record-keeping systems for confidential information (such as corporate employee departmental affiliations, project billing codes, etc.) now stored routinely in the CRS/GDS, but not essential to flight reservations or ticketing. The likelihood is that the costs of developing, deploying, and maintaining such systems, and their inefficiency relative to integrated large-scale systems like the CRS's/GDS's, would be catastrophic for many struggling small travel agencies.

Even the largest and most technically sophisticated Internet travel agencies do not yet have systems in place to notify travellers and obtain their consent for transfer of their personal data to CRS's/GDS's, to allow travellers to know which data elements are transferred to a CRS/GDS, or to control which data is stored in PNR's and which is stored elsewhere.

I've had extensive discussions over several years on this issue, for example, with the chief privacy officer of Expedia.com, formerly a division of Microsoft, which depending on the ranking criteria is either the largest or second-largest Internet travel agency, and one of the ten largest travel agencies, in the USA.

Despite a privacy policy that "Expedia.com believes that members and site visitors should have control over the collection and use of their PII [Personally Identifiable Information]", there is no way to determine from Expedia.com what data will be or has been transferred to what, if any, CRS/GDS, or at what point in the purchase process that transfer has occurred or will occur.

In fact, I have never encountered, in my extensive research, any Internet travel agency or airline Web site that actually enables users to know at what point in the process of researching, reserving, pricing, and purchasing air tickets a PNR will be "ended" (travel industry jargon for "saved" in standard computer usage), and information irretrievably transferred to a CRS/GDS.

So implementing systems to notify customers of the potential disclosure of their PNR data to the Department under these proposals, and to obtain their prior consent, will be nontrivial.

Even if the proposed ASSR system is not exempted from the Privacy Act, and is not found to be irreconcilable with the Canadian Personal Information Protection and Electronic Documents Act and the EU Data Privacy Directive (as it probably would be), all entities handling air travel data would be required as a result of the proposals to implement systems for notice and consent to disclosure of travel data, and recording and tracking of notice and consent to disclosure in PNR's and other records. This notice, consent, and record-keeping is desirable, long overdue, and -- as the examples of Canada and the EU make clear -- need not be overly costly if implemented gradually, with careful planning and cooperation between the privacy community, the travel industry, and regulators. But this cannot be implemented overnight, as contemplated by this proposal, and attempting to rush it into effect would greatly increase its costs.

Currently, there is no standard field in a PNR in any major CRS/GDS to indicate whether the subject of the data in the PNR has consented to disclosure of any or all of the data concerning them, or whether any of the subjects of the data in the PNR are subject to Canadian or EU jurisdiction and privacy regulations.

Nor could that be inferred from other data in the PNR: while a PNR might indicate the nationality of the travel document being used by a passenger for a particular journey, they might be a dual national also subject to the jurisdiction of another country, without that being mentioned in the PNR. And while a PNR might indicate the country of the billing address of the credit card used as the form of payment for tickets, or the address of delivery of the tickets (if paper tickets were issued), neither of those is dispositive of a person's country of legal residence, or physical location at the time of sale, which are more likely to determine jurisdiction -- and which, in most cases, are never known to the airline, CRS/GDS, or often even the travel agent.

An airline, CRS/GDS, or airline hosting company thus cannot currently "share" any PNR data voluntarily with the Department, without risk of violating a contractual non-disclosure agreement under which the information was provided by the traveller or a travel agency, or without risk of disclosing personal data of a Canadian or EU subject without their knowledge or consent, in violation of the obligations it has assumed as a condition of accepting business from persons subject to Canadian or EU law.

So in order to implement any "sharing" or disclosure of PNR data, consistent with airlines' and CRS's/GDS's contractual non-disclosure commitments to some customers and their obligations under Canadian and EU law not to disclose information on subjects of those countries' laws without notice and consent, recorded in the record, airlines and CRS's/GDS's would first have to add fields to each PNR to record whether the subject of the PNR is subject to the jurisdiction of the EU or Canada or another country whose laws require notice and consent for disclosure of personal information; whether that person has been notified and consented to disclosure of information to the department for inclusion in the ASSR system; and whether data in the PNR has been provided under a contractual commitment of non-disclosure.

Any airline, CRS/GDS, airline hosting system, or travel agency sharing PNR data with the Department, without making changes to its data model to enable it to exclude records protected by EU or Canadian law, or by privacy contracts, would risk catastrophic liability for breach of privacy and breach of contract.

Addition of entirely new fields to PNR data models is a slow and expensive process. So far as I know, the last time changes were made to a CRS's/GDS's data structure to enhance privacy

protection was in April of 2002 when, in response to my criticisms of the disclosure of PNR data over the Internet without a password, Sabre (the largest CRS/GDS), began using the contents of the "passenger e-mail address" field in the Sabre PNR as a pseudo-password for access to Sabre PNR data through Sabre's "Virtually There" Web gateway at <http://www.virtuallythere.com>. (See <http://hasbrouck.org/articles/watching.html>.)

This process took about two and a half months, even though it involved only adding a new function for the contents of an existing PNR field. Mr. David Houck, Sabre's Vice President, Industry Affairs, and chief privacy and regulatory compliance officer, told me in an interview that the reason Sabre chose to use the e-mail address as a pseudo-password, rather than a password stored as a separate field in the PNR (which would have been more secure, and standard data security and privacy practice in other industries), was that adding a new field to each PNR would take substantially longer and be prohibitively expensive.

Further indication of the potential cost of compliance with this proposal is contained in the comments of the International Air Transport Association (IATA) on the INS "Notice of Proposed Rulemaking on Manifest Requirements", Docket No. INS 2182-01, RIN 1115-AG57, comments dated 3 February 2003. The INS proposal is at <http://www.ins.usdoj.gov/graphics/lawsregs/fr010303.pdf> and a copy of IATA's comments is available online at <http://www.epic.org/privacy/airtravel/iata_ins_pax_manifest.pdf>.

According to these recent comments by IATA, the direct costs to the airlines alone of implementation of a system to provide the Federal government with post-departure batch access (not real-time or continuous access) to passenger manifest information (limited to a small finite number of specified data fields, not the entire PNR), for international flights only (not all flights), would be "significantly higher" than IATA's initial "extremely conservative" estimate of US$164 million. The cost of implementation of the ASSR proposals at issue in this rulemaking proceeding would undoubtedly be substantially higher still.

As this discussion has already made clear, the information included in PNR's, and apparently intended to be included in the proposed ASSR system, would not be limited to data about individuals, but would include detailed insider information about businesses of all sizes and their activities, from how much time

specific employees spend with each other to which people are authorized to approve expenditures of what amounts on what projects or under which accounting codes.

For all these reasons the proposal should be withdrawn at least until the Department has conducted the requisite analysis of its impact as a significant regulatory action, particularly given its likely immense economic impact and its likely critical direct impact on tens of thousands of small travel businesses, and taking into consideration the fundamental incompatibility of the proposals, particularly if exempted from the Privacy Act, with the Canadian Personal Information Protection and Electronic Documents Act and the EU Data Privacy Directive.

That analysis should include public hearings and expert and public testimony on the potential impact of the proposals, particularly on individual privacy, confidentiality of business information, personal and business data handling by small and large online and offline travel agencies, and related impacts on personal information practices in the travel industry.

Given the significance to the economic impact of the proposals of their harmonization (or lack thereof) with Canadian and EU privacy regulations, that analysis should also involve representatives of the Office of the Privacy Commissioner of Canada and the European Union Data Privacy Commission.

5. THE PROPOSED SYSTEM OF RECORDS AND ITS USES WOULD BE UNCONSTITUTIONAL.

The First Amendment to the U.S. Constitution provides that, “Congress shall make no law ... abridging ... the right of the people peaceably to assemble.”

Few activities implicate the assembly clause of the First Amendment as directly as travel. When people travel to assemble, as they do when they travel for business or organization meetings or conventions, or to meet friends and relatives, their travel is an act of assembly. Travel is not just an activity often engaged in for purposes protected under other clauses of the First Amendment (such as travel to petition the government for a redress of grievances, or travel for purposes protected as freedom of speech or of the press), but travel is, in and of itself, an activity directly protected under the assembly clause of the First Amendment.

Statutory or regulatory measures potentially abridging the right of the people peaceably to travel must therefore be evaluated in accordance with the strictest standards applicable to measures infringing on directly-protected First Amendment activity.

In a country as large and discontiguous as the USA, air travel is particularly essential to the exercise of the First Amendment right of the people to assemble. Even within some states, such as between islands of Hawai'i and between many parts of Alaska, there is no meaningful or affordable alternative to air transportation. In the USA today, no national assembly of people, for any purpose, is feasible without air transportation.

Thus a law restricting access to air transportation, or permitting some people to be denied access to air transportation, is clearly a "law ... abridging ... the right of the people peaceably to assemble", and must be evaluated accordingly.

As noted above, it appears from the invocation of 49 U.S.C. 114 as statutory authority for the proposed system of records that the ASSR system might be used under subsection (h)(3) as the basis to "prevent the individual from boarding an aircraft".

Absent a showing that such use of information from the proposed system of records would satisfy the standard for an exception from the First Amendment protection of the right to assemble, the proposal should be revised to specify that no information from the system will be used as the basis for the denial of transportation to any otherwise qualified individual.

Failing that, the proposal should be modified to include sufficient due process, with respect to any data which might be used as the basis of a decision to deny transportation, to satisfy the requirements for the determination of an exception to an individual's First Amendment right to assemble.

The "Notice To Amend A System Of records" contains no such due process. The "Contesting Record Procedures" in the notice contain no meaningful due process provisions. And those procedures in the proposal apply only to information provided by the subject of the record, not to information provided by third parties. Very little of the information in the proposed ASSR system would be provided directly by the subjects of the records in the system: air travellers (except travel agents and airline

staff arranging their personal travel) almost never enter data directly in their own PNR's. Most PNR data is provided by travel agents and airline staff, and most of the other categories of data proposed to be included are provided by other third parties.

The proposed exemption of the proposed record system from the Privacy Act, by making it impossible for an individual to determine whether they are the subject of a record being used as the basis for restricting their right to assemble by means of air travel, or to determine what data in the system is being used as the basis for that restriction of the right to assemble by means of air travel, is incompatible with the requisite due process.

If the proposed system of records is to be used as the basis for any action under 49 U.S.C. 114 (h)(3)(B), the proposal to exempt the system of records from the Privacy Act should be withdrawn.

Respectfully submitted,

Edward Hasbrouck

San Francisco, CA, USA
23 February 2003

This document is also available on the Web at:

http://hasbrouck.org/articles/
Hasbrouck_DOT_comments-23FEB2003.pdf