

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 (3rd edition, forthcoming 2004)

<http://www.practicalnomad.com>

30 September 2003

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528, USA
privacy@dhs.gov

COMMENTS OF EDWARD HASBROUCK RE: DOCKET NUMBER DHS/TSA-2003-1, “PASSENGER AND AVIATION SECURITY SCREENING RECORDS” (PASSR)

Privacy Act of 1974, “Notice of status of system of records; Interim final notice; Request for further comments”, Records System DOT/TSA 010, 68 *Federal Register* 45265-45269, 1 August 2003, <http://www.dhs.gov/dhspublic/interweb/assetlibrary/CAPPSII_PRIVACY_ACT_NOTICE.pdf>

ABSTRACT:

=====

1. The “Supplementary Information” published in conjunction with this Privacy Act Notice (“the Notice”), and the Notice itself, materially misrepresent the content of the Notice, the nature of the proposed “CAPPS-II” system, and the public comments submitted in response to the Department of Transportation’s earlier Privacy Act Notice for this records system:

A. The Department of Homeland Security (“the Department”) has failed to acknowledge, or to modify the proposal in response to, most of the comments filed in response to the prior Notice, despite the false claim to the contrary in this Notice.

B. The "Supplementary Information" published in conjunction with the Notice includes false and misleading statements about material aspects of the proposal, as specified in the Notice itself, and misstates the personal information collection practices of airlines and the travel industry.

C. The Notice omits from its description of "Categories of Individuals Covered by the System" large categories of individuals about whom the system, as described in the Notice, would contain personally identifiable information.

2. The proposed "Computer Assisted Passenger Screening System, version 2" (CAPPSS-II) and "Passenger and Aviation Security Screening Records" (PASSR) systems, as described in the Notice, violate the assembly clause of the First Amendment, and the Constitutional right to travel, and are unconstitutional.

3. The proposed "CAPPSS-II" and "PASSR" systems are contrary to the express requirements of Federal statutes:

A. The Notice is contrary to the Privacy Act of 1974, 5 U.S.C. 552a(e)(7), which prohibits the maintenance of records concerning how individuals exercise rights guaranteed by the First Amendment (specifically, in this case, the right to assemble, as well as other rights).

B. The Notice is contrary to the letter and the intent of the Airline Deregulation Act of 1978, 49 U.S.C. 40101.

4. The proposed "CAPPSS-II" and "PASSR" systems are not authorized by any of the statutes cited as authority for the maintenance of the systems. Among other things, the Department has failed to make the showing of "necessity" required by 49 U.S.C. 114(1)(1), which would require showing that no less burdensome alternative could serve any valid purpose of the proposed regulations.

5. The Department has (still) failed to consider numerous factors and conduct numerous assessments required by statute to be considered in prescribing such a regulation, including whether the costs are excessive in relation to any enhancement of security, whether it is consistent with protecting passengers, whether it is consistent with the public interest in promoting air transportation, and the extent, if any, to which it will actually be effective to protect passengers and property.

6. The Department has failed to comply with the procedural and substantive notice requirements of the statutes claimed as authority for the proposals, or of the Privacy Act of 1974.

A. The Department has failed to comply with the requirement 49 U.S.C. 44901(h)(2) that Congress be advised at least 30 days prior to the effective date of any regulation issued under the authority of 49 U.S.C. 44901. As published, there is no prior notice at all: the Department apparently intends to apply the Notice retroactively to reservation records (PNR's) that have already been created.

B. The Department has failed to notify those who are asked to supply information what information is being requested, the authority for the solicitation of information, whether providing the information is mandatory or voluntary, and the effects of not providing any part of the requested information, as required by the Privacy Act of 1974.

COMMENTS:

=====

About the Author:

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.

About these Comments:

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 "SUPPLEMENTARY INFORMATION" PUBLISHED IN CONJUNCTION WITH THIS PRIVACY ACT NOTICE ("THE NOTICE"), AND THE NOTICE ITSELF, MATERIALLY MISREPRESENT THE CONTENT OF THE NOTICE, THE NATURE OF THE PROPOSED "CAPPS-II" SYSTEM, AND THE PUBLIC COMMENTS SUBMITTED IN RESPONSE TO THE DEPARTMENT OF TRANSPORTATION'S EARLIER PRIVACY ACT NOTICE FOR THIS RECORDS SYSTEM.

A. The Department of Homeland Security ("the Department") has failed to acknowledge, or to modify the proposal in response to, most of the comments filed in response to the prior Notice, despite the false claim to the contrary in this Notice.

In the section of the Notice on "Public Comments", the Department claims that, "TSA respects the concerns raised by commenters, and has modified the proposed system of records to address many of these concerns." But that's not true. Only minor changes have been made in response to a few of the comments; most of the changes make the proposal even more objectionable to most commenters; and most of the comments have been entirely ignored.

The Notice fails even to acknowledge the existence, much less respond to, any of the hundreds of comments objecting to the prior Notice on the grounds that it is unconstitutional; that it violates the right to travel; that the proposal exceeds the claimed statutory authority; that the issuing agency (the Department of Transportation, whose authority was transferred to the Department of Homeland Security while the proposal was pending) had failed to consider factors required by statute to be considered; that the issuing agency had failed to conduct the required analysis of regulatory impacts (including the economic impact, impact on small business, and impact of the incompatibility of the proposal with the data protection and privacy laws of major air transportation partners of the USA, including the European Union and Canada); and that the earlier notice failed to satisfy the statutory notice and comment requirements.

The Department also claims in the Notice that, "The comments and concerns raised will continue to be considered during the testing and evaluation periods". But there is no evidence in the Notice, or in the Department's actions to date, that those concerns have even begun to be considered.

If the Department genuinely respected the concerns raised by commenters, or was willing to consider meaningful changes to the proposal to address those concerns, the Department would have worked with commenters to formulate those changes. But the Department did not do so. There has been no forum open to the public for input into the proposal (except for the opportunity to file formal comments, to which the public has responded with an overwhelmingly flood of almost unanimously negative comments). Even commenters such as myself, who were individually promised in writing that we would be invited to meet with representatives of the Department prior to the finalization of this revised Notice, were never actually given any opportunity to do so.

The Notice also asserts that, "The Department of Homeland Security is committed to working with airlines and the travel industry to provide greater understanding and awareness of the purposes for the scope of CAPPS-II." But despite that professed "commitment", the Department has thus far made no attempt whatsoever to work with any of the commenters on the CAPPS-II proposal from within the airline and travel industry.

Only 2 of more than 200 comments on the earlier Notice came from parties within the travel industry: my comments and those of British Airways, made through their legal counsel in the USA. As noted above, the Department promised me in writing in March 2003 that I would be invited to their next CAPPS-II "stakeholder" meeting, but that promise has not yet been fulfilled. I don't know whether no such meeting has been held, or whether it was held but the Department broke their promise to invite me to it.

The comments from British Airways concerned the conflicting demands placed on them by the Department's proposal and by the data protection requirements of other countries, particularly the United Kingdom and the European Union. Those concerns, like those in my comments, are entirely ignored in the most recent Notice, suggesting that the Department hasn't been "working with" British Airways either.

If the Department hasn't even talked to, or acknowledged the concerns of, those within the airline and travel industry who filed formal comments on the earlier Notice, it's not clear why the Department's professed commitment to working with airlines and the travel industry should be given any credibility.

B. The "Supplementary Information" published in conjunction with the Notice includes false and misleading statements about material aspects of the proposal, as specified in the Notice itself, and misstates the personal information collection practices of airlines and the travel industry.

The "Supplementary Information" published with the notice goes far beyond mere "spin doctoring". At minimum, it is an attempt to mislead the public on this issue of great public concern. To the extent that the Notice in the *Federal Register* is intended to constitute the notice to Congress required by 49 U.S.C. 44901(h)(2), it is also an attempt to defraud the Congress.

The false and misleading claims about the Notice, as it is mis-described in the "Supplementary Information" that accompanied the Notice, include the following:

(1) "This system notice reduces the extent to which TSA will maintain or disseminate personal information on airline passengers."

In fact, the Notice substantially expands the information that the TSA would receive and be able to disseminate. In the earlier Notice, the information obtained from travel industry sources would have been limited to Passenger Name Records (PNR's), with whatever data they might contain. The revised Notice would require PNR's to contain additional data which is not needed for any business purpose, is not required or even optionally provided for by any industry standard, and is absent from almost all current PNR's – substantially expanding the scope of the proposal, and dramatically increasing the burden it imposes on the travel industry and the cost to the industry of compliance.

(2) "[T]he CAPPS-II system, when active, will maintain only the routine information that all individuals provide when making reservations, as contained in the PNR, including full name, date of birth, home address and phone number."

None of this information is necessarily present in current PNR's (some of it is almost never present), and none of it can accurately be described as "routine":

(a) Not all airline passengers make reservations prior to travel, or make reservations at all.

Many passengers travel on unreserved shuttle services, at "walk-up" fares or on "open" tickets that do not require reservations, as standby passengers without reservations, or on flight other than those on which they held reservations.

- (b) Group reservations are routinely made with no names at all. Names may be added to group reservations long after they are made, or at the time of the flight, or not at all.
- (c) "Full" names (whatever that might mean) are never required. Limitations of airline reservation hosting systems, computerized reservation systems (CRS's), and interline messaging systems and protocols, limit both the permissible character set and the length of the name in which a reservation can be made. Hyphens, apostrophes, and diacritical marks, for example, are not permitted in most reservation systems, and spaces are generally not permitted within surnames. Some people can never use their "full" names in reservations, even if they want to: people with long or hyphenated names; people with spaces within their surnames; people with names that contain apostrophes or diacritical marks; and people whose names in their full form are written in alphabets or character sets other than the Latin alphabet. Finally, under current law in the USA, one can use any name one wishes, as long as one does so without intent to defraud, so there is no expectation or requirement that the same individual's "full" names at different times or in different PNR's will be the same.
- (d) Date of birth is almost never included in a PNR; it can't possibly be called "routine".
- (e) "Home address" (whatever that might mean, since many people have more than one address, and some people, especially perpetual travelers, have no home — I know road warriors who spend 365 nights a year as guests of hotels, friends, or family) is not required by any airline, and is rarely included in PNR's. At most, one address is

entered in a PNR, regardless of the number of passengers in the PNR. Industry standards such as the AIRIMP recognize this in providing for a sole "lead contact" for each PNR. If there is any address in a PNR, it is most often an address of a travel agency, not an address of any of the passengers.

(f) "Home phone number" (again, whatever that might mean, when some people have no phone, others have no land line, and an increasing number of cell phones and Voice-Over-IP phones have no particular association with a "home" or any physical location) is not required by any airline, and is rarely included in PNR's. Some airlines require a phone number in each PNR, but none require separate phone numbers for each passenger, or require that any phone number correspond to a "home". If there is a phone number in a PNR, it is most often that of a travel agency. And if there is a passenger phone number in a PNR, it is at least as likely to be a cell phone, business, hotel, voicemail, or other number at which a passenger might be contacted while travelling as it is to be a passenger's "home" phone number.

(3) "TSA will obtain electronically, either from airlines or from Global Distribution Systems, a passenger's 'passenger name record' (PNR) as collected from the passenger by a reservation system."

Contrary to this scenario, information in PNR's is almost never collected directly from the passenger by a reservation system. That typically happens only when airline, travel agency, or CRS staff make reservations for themselves for their personal travel. In most cases, there are multiple intermediaries between the passenger and the transporting airline's host system or CRS. In order to comply with this notice, each of those intermediaries would have to collect, store, and forward each of the data elements required under this Notice, and would have to modify their internal systems and their interfaces with passengers, airlines, CRS's, and other intermediaries to support the collection, storage, and forwarding of those data elements.

[Note that what are referred to in the Supplementary Information as "Global Distribution Systems" (GDS's) are also referred to – in the Notice itself, in the Department of Transportation regulations under which they operate, and in the travel industry – as "Computerized Reservation Systems", or CRS's.]

- (4) "PNR includes the routine information collected at the time a passenger makes a flight reservation."

Actually, a PNR almost never consists exclusively of information collected at the time a reservation is made (even assuming a reservation is made by the passenger, rather than by a family member, business associate, travelling companion, travel agent, group coordinator, or other intermediary, as is the case for the majority of passengers). Confirmation codes and messages returned after the reservation is made, changes and additions to the reservation, requests for seating assignments or other services and responses to those requests, ticketing information (usually a PNR is created and saved before a ticket is issued), and a wide variety of other information is routinely added to the PNR between the time the PNR is created and the time of travel.

This fact makes it particularly unclear which portion, if any, of the information proposed to be required by the Notice must be present in the PNR at the time of creation of the PNR, or by exactly what time, between then and the time of travel, the required information must have been added to the PNR, highlighting the substantive notice deficiencies of the Notice.

- (5) "A PNR may include each passenger's full name, home address, home telephone number, and date of birth."

This may be the most economically significant of all the misstatements in the Supplementary Information and the Notice. In reality, most PNR's cannot now contain all this information, because current PNR formats, data structures, and interline data interchange and messaging protocols do not support these additional (currently optional, and some rarely used) data items.

It's not clear whether the Department has developed the CAPPS-II scheme in isolation from, and in ignorance of, how airline passenger information is handled, or whether the Department is knowingly trying to mislead the public and the Congress about the likely total cost of this proposal.

The Department's budget of US\$35 million in 2004 for completion of development, testing, and deployment of CAPPS-II is ludicrously inadequate for this task. As I discussed in detail in my comments on the original Notice, the International Air Transportation Association (IATA) estimated earlier this year, in comments filed on a parallel but much more limited proposal by the INS (now also part of the Department of Homeland Security), that the cost of providing much more limited access to a smaller subset of PNR data on international flights only would be "significantly higher" than IATA's initial "extremely conservative" estimate of a US\$164 million. That proposal would have involved information collected from passengers directly by the airlines at check-in, so it would not have required any changes by travel agencies, CRS's, or any other intermediaries.

Either the Department is completely clueless about the implications of this proposal, and doesn't yet realize what sweeping changes in airline industry information technology infrastructure, protocols, and interfaces this proposal would require. Or the Department does know, and intends to impose implementation costs of US\$1 billion or more on an airline industry that can ill afford them, and that will be obliged to pass them on to passengers in the form of higher fares.

In response to a Freedom of Information Act lawsuit by the Electronic Privacy Information Center, the Department has said that its business case and economic and privacy impact assessments are still not complete, and the Department has withheld them in their entirety from public disclosure.

The seriousness of the Department's misconceptions as to industry practices strongly suggests that those assessments are based on such ignorance and fallacies as to render them worthless as a basis for evaluating the proposal. Consequently, *de novo* economic and privacy impact assessments should be made by the Office of Management and Budget and the General Accounting Office, and other appropriate oversight bodies such as Congress itself.

(6) "The commercial data providers ... will not acquire ownership of the data, nor will they be permitted to retain the data in any commercially usable form. TSA will not permit the commercial data providers to use this data for any purpose other than in conjunction connection with the CAPPS-II program."

The untruth in this claim is partly just obfuscation: commercial data providers don't need to "acquire" ownership of PNR data, since under the law in the USA they already own PNR data from the moment of PNR creation. PNR's and other records about travellers currently belong to commercial data providers – CRS's, travel agencies, and/or airlines – and don't belong to travellers.

That's bad enough, but what's worse is the out-and-out lie in the Supplementary Information in the claim that the Notice restricts ownership, usage, retention, or disclosure by commercial data providers of any of the data in this system. It's not just that the Notice doesn't – as the Supplementary Information appears to claim – transfer ownership of PNR's to the TSA or the Department (which would, in any case, create more privacy problems that it would solve). This whole section of the Supplementary Information refers to alleged provisions of the Notice that simply don't exist! If the Department's intention is to provide such restrictions on commercial use of PNR data, that should be included either in the Notice itself, and/or in the Department of Transportation's CRS regulations. It is not. The CRS regulations are currently under review and revision by the DOT, but neither the current regulations nor any of the proposed changes include any consumer privacy provisions or protections.

C. The Notice omits from its description of "Categories of Individuals Covered by the System" large categories of individuals about whom the system, as described in the Notice, would contain personally identifiable information.

As I discussed in detail in my comments on the earlier Notice for this system, PNR's contain personally identifiable information on several categories of individuals other than air travellers. These other categories of individuals are overlooked by the department in the Notice – further evidence of the Department's apparently complete ignorance of what's actually in a PNR.

Under 5 U.S.C. 552a(a)(e)(4)(B), a Privacy Act Notice in the *Federal Register* must disclose the categories of individuals on whom records are maintained in the system. Thus, for this reason alone, the Notice must be republished, fully disclosing the categories of individuals about whom PNR's contain information, before any PNR's can be transferred to the Department.

Among those categories of individuals about whom PNR's, and thus the system as described in the Notice, would contain information, but which are not mentioned in the Notice, are the following:

- (1) Individuals who make reservations for air travel, but who do not actually travel, and who never purchase tickets and/or cancel their reservations.

A large percentage of PNR's are cancelled, in most cases before tickets are ever issued. If PNR's are transferred to the Department at any time prior to flight departure, they will inevitably contain PNR's for individuals who don't end up on the flight. To be accurate, the Notice should be broadened to give notice that the system may include information on anyone for whom an airline reservation is made – with or without their knowledge, and whether or not they actually purchase tickets or travel.

Of course, that wouldn't be necessary if information were transferred only at the time of flight departure. But in that case, there would be no need to conscript so many intermediaries as data collection agents of the Department. The Department's own TSA staff could collect any required information directly from passengers at security checkpoints at airports, in accordance with the Privacy's Act's statutory preference for collection of information, to the greatest extent practicable, directly from the data subject by the government.

- (2) Travel arrangers, personal assistants and administrative staff, travel managers, group coordinators, event organizers, and family members and friends assisting with travel arrangements, as identified by the "received from" field in the "history" (audit trail) for each PNR entry that records the person who requested the reservation or change.

The Notice should be broadened to give notice that the system will include information on anyone who requests that a reservation be made or altered, even for someone else.

- (3) People who pay for tickets for others, or who hold joint credit or debit cards with people who purchase travel for themselves or others – again, whether or not they travel themselves – as identified from the "form of payment" fields in ticketing records in PNR's.

The Notice should be broadened to give notice that the system will include information on anyone who pays for airline tickets or who holds a joint account with someone who pays for tickets.

(4) Travel industry personnel, including travel agents and airline reservation, check-in, and ticketing staff, as identified by the unique "agent sine" or log-in ID in the PNR "history" for each entry or change and by 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 or airline hosting system counterpart of an Internet IP address).

PNR's 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. The Notice should be broadened to give notice that the system will include information on all such personnel.

Given the level of transactional detail about the activities of front-line travel agency and airline reservations, ticketing, customer service, check-in, and gate staff contained in the PNR's with which they work, these would actually be the individuals about whom the proposed system would contain the most information, and with respect to whom the deficiency in the Notice could be seen as most significant.

(5) Clients, customers, and employers of travellers, even if they aren't travelling, as identified by billing and accounting codes for travel by others undertaken on their behalf or at their expense.

It is particularly critical that the Department give notice before starting to collect any such information, since in many cases it is 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 are routinely the subject of data in PNR's, and thus could be the subject of data in the proposed system.

2. THE PROPOSED "COMPUTER ASSISTED PASSENGER SCREENING SYSTEM, VERSION 2" (CAPPS-II) AND "PASSENGER AND AVIATION SECURITY SCREENING RECORDS" (PASSR) SYSTEMS, AS DESCRIBED IN THE NOTICE, VIOLATE THE ASSEMBLY CLAUSE OF THE FIRST AMENDMENT, AND THE CONSTITUTIONAL RIGHT TO TRAVEL, AND ARE 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. Travel is, in and of itself, in most cases, 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.

Accordingly, the Department either must make clear that the proposed CAPPS-II and PASSR systems cannot and will not be used as the basis for any denial of transportation, or must justify those systems under the strict standards applicable to systems

which might be used as the basis for regulation of an activity – to wit, assembly – directly protected by the First Amendment.

The Department has done neither, and the proposed Notice must therefore be withdrawn, or voided by appropriate oversight authorities or a Court of appropriate jurisdiction.

3. THE PROPOSED “CAPPSS-II” AND “PASSR” SYSTEMS ARE CONTRARY TO THE EXPRESS REQUIREMENTS OF FEDERAL STATUTES.

A. The Notice is contrary to the Privacy Act of 1974, 5 U.S.C. 552a(e)(7), which prohibits the maintenance of records concerning how individuals exercise rights guaranteed by the First Amendment (specifically, in this case, the right to assemble, as well as other rights).

According to the Privacy Act of 1974, 5 U.S.C. 552a(e)(7), “Each agency that maintains a system of records shall... (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.”

As discussed above, most acts of air travel are acts of assembly directly protected by the First Amendment. If the complete contents of all air travel reservations aren’t “records concerning how individuals exercise” their right of assembly, as guaranteed by the First Amendment, I don’t know what is.

Travel records show when people assemble, where (and from where) they assemble, with whom they assemble, what activities they engage in during their assemblies, and numerous other details of exactly how they exercise their right of assembly.

None of the exceptions in 5 U.S.C. 552a(e)(7) applies to the records sought to be maintained under this Notice. Any arguable statutory authorization for the maintenance of any of the travel records described in this proposal is, at best, implicit, and does not meet the statutory requirement that it be “expressly” authorized. And the Notice does not concern a law enforcement activity at all, much less limit itself to such an activity.

49 U.S.C. 44903(h)(2) requires that “The Secretary of Transportation shall insure that the Computer-Assisted Passenger

Prescreening System, or any successor system – (i) is used to evaluate all passengers before they board an aircraft.”

The Secretary of Transportation is required to ensure that CAPPS (or its successor) is used, but that statutory obligation could be fulfilled by regulations or directives requiring that CAPPS be used by airlines or commercial screening firms. There is no statutory requirement that CAPPS be used or operated by the government itself, or that its operation entail any transfer of data to, or maintenance of records by, any government agency.

And the mandate to use “[CAPPS] or any successor system” cannot be construed as an open-ended mandate – and most especially not as the “express” authorization” required by the Privacy Act – for any new and different system which the Department may later chose to label as CAPPS-II, CAPPS-3, or CAPPS-Infinity.

The only other statutory reference to CAPPS is in 49 U.S.C. 44901: “... [S]creening ... shall be carried out by a Federal Government employee ... except for identifying passengers and baggage for screening under the CAPPS and known shipper programs in conducting positive bag-match programs.” By explicitly excepting CAPPS from any mandate of Federalization, this clause makes even more clear the express Congressional intent not to require any Federal role in the operation of the CAPPS system.

Since the records proposed to be maintained described how individuals exercise rights guaranteed by the First Amendment, and since no such maintenance of records is expressly authorized by statute, creation or use of the proposed system of records is expressly barred by the Privacy Act. The proposed Notice must therefore be withdrawn, or voided by appropriate oversight authorities (including the Department’s Chief Privacy Officer, as oversight officer responsible for the Department’s compliance with the Privacy Act) or by a Court of appropriate jurisdiction.

B. The Notice is contrary to the letter and the intent of the Airline Deregulation Act of 1978, 49 U.S.C. 40101.

The Airline Deregulation Act of 1978, 49 U.S.C. 40101(a), requires the Secretary of Transportation (whose obligations, to the extent they are relevant to these proposals, have been transferred to the Secretary of Homeland Security) to “consider the following matters, among others, as being in the public interest and consistent with public convenience and necessity:”

“(6) placing maximum reliance on competitive market forces and on actual and potential competition—

(A) to provide the needed air transportation system...

“(12) encouraging, developing, and maintaining an air transportation system relying on actual and potential competition—

(A) to provide efficiency, innovation, and low prices; and

(B) to decide on the variety and quality of, and determine prices for, air transportation services.”

In addition, the Airline Deregulation Act at 49 U.S.C. 40101(e) requires that the “Secretary of Transportation shall ... emphasize[e] the greatest degree of competition compatible with a well-functioning international air transportation system, including the following:

“(2) freedom of air carriers and foreign air carriers to offer prices that correspond to consumer demand....

“(5) eliminating operational and marketing restrictions to the greatest extent possible.”

Implicit in this Notice are a variety of operational, marketing, and especially pricing restrictions on both domestic and international air transportation that are directly contrary to these statutory provisions.

Fare rules and conditions are an essential element of airline pricing. (By definition, under IATA and DOT rules, a “fare” is a price associated with specific rules.) By requiring reservations as a condition of airline travel, the proposed systems would apparently forbid, among other industry practices:

(1) the offering of fares that do not require reservations

(2) the operation of unreserved shuttle or walk-on services

(3) the sale or use of “open” tickets, which by definition do not require reservations

- (4) carriage of "stand-by" passengers not holding reservations
- (5) acceptance of group reservations without individual names
- (6) structuring of reservation data in formats other than Passenger Name Records (PNR's); for example, as tables in a relational database rather than records in a "flat database" (all 4 major CRS's currently use flat, not relational, databases, and a "PNR" is by definition a record in such a "flat" database)

According to the Section 2.1.7 of the IATA General Rules (as published in the *Passenger Air Tariff*), and the Conditions of Carriage of every major airline in the USA and most airlines in the world, tickets are valid on any flight satisfying the routing and other rules of the fare, for 1 year from the date of issue (or in specified cases 1 year from the date of commencement of travel). Advance reservations are not required for "normal" fares, but are required only if that is a condition of a "special" fare (IATA General Rules, Sections 2.1.5.1-2.1.5.2).

Many fares are special fares with rules requiring advance reservations, but many tickets are still issued at normal fares, or at special fares that don't have advance reservation requirements. Many air travellers use unreserved shuttle services or "open" tickets, or stand-by to travel without reservations.

In effect, this Notice seeks to impose a reservation requirement (and perhaps, although the Notice is too vague to tell, an advance reservation requirement of some specific amount of time), as a condition of all fares to be offered by all airlines for any portion of any journey that touches the jurisdiction of the USA.

To the extent that it is applied to any flights operated less than 1 year after the final Notice, it also seeks, apparently, to impose such a reservation condition retroactively on tickets already issued, and valid for another year or more, that carried no such requirement at the time of issue. Airlines and travel agencies do not necessarily have any way to contact ticket holders while they are travelling. Holders of such tickets have no way to know that the conditions of their tickets have been changed until they present themselves for check-in and discover that they cannot travel without reservations.

The industry trend has been toward the elimination or reduction of advance-reservation requirements. And all major CRS's are working toward the fundamental restructuring of reservation data in more efficient ways that might eliminate the concept of the PNR. These are the sorts of changes that the Airline Deregulation Act was intended to encourage and facilitate.

The imposition of more restrictive government-mandated fare and ticket sales conditions, contrary to industry norms and counter to the industry trend toward less restrictive fare conditions, particularly with respect to advance reservations, is exactly the sort of anti-competitive regulatory activity that the Airline Deregulation Act of 1978 was intended and enacted to prohibit.

Finally, the Airline Deregulation Act at 49 U.S.C. 40101(c) requires that "the Administrator of the Federal Aviation Administration", (again, whose obligations have in relevant part been transferred to the DHS and TSA), "shall consider ... (2) the public right of freedom of transit through the navigable airspace."

There is no evidence of such consideration in the instant Notice, or in any of the Department's actions in this matter, nor even of any recognition by the Department of this Congressionally (and Constitutionally) recognized right of freedom of travel. The proposal must be withdrawn until the Department has considered its impact on the "public right of freedom of transit through the navigable airspace", as specifically required by this statute.

4. THE PROPOSED "CAPPS-II" AND "PASSR" SYSTEMS ARE NOT AUTHORIZED BY ANY OF THE STATUTES CITED IN THE NOTICE AS AUTHORITY FOR THE MAINTENANCE OF THE SYSTEMS.

The statutes cited in the Department's revised Notice as authority for the CAPPS-II and PASSR systems are the same statutes cited in the DOT's original notice for the ASSR system.

In my comments on the earlier Notice, I analyzed in detail each of the cited statutes, and the ways in which it falls short of authorizing the proposed systems.

That analysis in my comments was entirely ignored in the Department's revised Notice, and in the section of the "Supplementary Information" that purported to discuss the public

comments on the earlier Notice. No changes were made to the proposals that would bring them within the statutory authority.

Among other things, the Department has still failed even to attempt to make the showing of "necessity" required by 49 U.S.C. 114(1)(1) for regulations issued under authority of Section 114, which would require showing that no less burdensome alternative could serve the statutory purpose of the proposed regulations.

Accordingly, I reiterate, and hereby incorporate by reference, in their entirety, my comments on the earlier proposal and Notice. (A copy of those comments is also attached to this filing, as an integral part of this document and these comments.)

Since this proposal is broader than the original proposal, it goes even further beyond the Department's statutory authority.

As I pointed out in my previous comments, the cited statutes authorize the use of different sub-sets of PNR data by different divisions of what is now the Department for different purposes – but not the particular data items by the particular agencies for the particular purposes contemplated by these proposals.

But it's no longer necessary to reach that argument, since the revised Notice purports to require the collection of data not now required or even common in PNR's ("full name, home phone number, home address, and date of birth"). Nothing in any of the cited statutes even arguably gives the Department the authority to mandate the collection and forwarding to the Department, through as many intermediaries as may be necessary, of such non-PNR data.

5. THE DEPARTMENT HAS (STILL) FAILED TO CONSIDER NUMEROUS FACTORS AND CONDUCT NUMEROUS ASSESSMENTS REQUIRED BY STATUTE TO BE CONSIDERED IN PRESCRIBING SUCH A REGULATION.

Among other failings, as was discussed in detail in my comments on the previous Privacy Act Notice (incorporated herein by reference, in their entirety, and attached hereto as an integral part of these comments), the Department has failed to consider the following statutorily required questions:

- A. "whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide", 49 U.S.C. 114(1)(3), which should include consideration of the costs to airlines, CRS's, travel

agencies (which are primary small businesses), and suppliers of air transportation software and information technology;

B. "whether [the] proposed regulation is consistent with ... protecting passengers", 49 U.S.C. 44903(b)(2)(A), which should include consideration of protection of passengers against identity theft, stalking, and privacy invasion;

C. "whether [the] proposed regulation is consistent with ... the public interest in promoting air transportation", 49 U.S.C. 44903(b)(2)(B), which should include the possible consequences of cessation of air services with countries with whose data protection laws the proposal is incompatible, including Canada and the European Union;

D. "the extent to which [the] proposed regulation will carry out this section", 49 U.S.C. 44903(b)(2)(B), i.e. the extent, if any, to which the proposed regulation will actually be effective to "protect passengers and property".

Since each of these factors are required to be considered before a regulation can be adopted under these statutes (which were cited as authority for the Notice), the Notice must be republished, including an assessment of each of these statutorily required considerations, and an opportunity provided for public comments on the Department's assessments.

Public notice and the opportunity for public comment are particularly significant with respect to these considerations, in light of the Department's ignorance of actual airline and travel industry information systems and business practices, as is evident from the Notice itself and from the Department's failure even to understand the comments filed on the previous Notice.

6. THE DEPARTMENT HAS FAILED TO COMPLY WITH THE PROCEDURAL AND SUBSTANTIVE NOTICE REQUIREMENTS OF THE STATUTES CLAIMED AS AUTHORITY FOR THE PROPOSALS OR OF THE PRIVACY ACT OF 1974.

A. The Department has failed to comply with the requirement 49 U.S.C. 44901(h)(2) that Congress be advised at least 30 days prior to the effective date of any regulation issued under the authority of 49 U.S.C. 44901. As published, there is no prior notice at all: the Department apparently intends to apply the Notice retroactively to reservation records (PNR's) that have already been created.

As discussed in my comments on the previous Notice for this system of records, which suffered from the same procedural notice deficiency, the Department has (still) failed to provide the notice to Congress, and the opportunity for Congressional oversight, required by the (allegedly) authorizing statute.

The lack of Congressional notice is even more significant now than it was at the time of the previous Notice. In the interim, Congress has enacted, and sent to the President for signature, H.R. 2555, the "Department of Homeland Security Appropriations Act, 2004", which includes the following provisions:

"SEC. 519.

"(a) None of the funds provided by this or previous appropriations Acts may be obligated for deployment or implementation, on other than a test basis, of the Computer Assisted Passenger Prescreening System (CAPPS II) that the Transportation Security Administration (TSA) plans to utilize to screen aviation passengers, until the General Accounting Office has reported to the Committees on Appropriations of the Senate and the House of Representatives that—

"(1) a system of due process exists whereby aviation passengers determined to pose a threat and either delayed or prohibited from boarding their scheduled flights by the TSA may appeal such decision and correct erroneous information contained in CAPPS II;

"(2) the underlying error rate of the government and private data bases that will be used both to establish identity and assign a risk level to a passenger will not produce a large number of false positives that will result in a significant number of passengers being treated mistakenly or security resources being diverted;

"(3) the TSA has stress-tested and demonstrated the efficacy and accuracy of all search tools in CAPPS II and has demonstrated that CAPPS II can make an accurate predictive assessment of those passengers who may constitute a threat to aviation;

“(4) the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which CAPPS II is being developed and prepared;

“(5) the TSA has built in sufficient operational safeguards to reduce the opportunities for abuse;

“(6) substantial security measures are in place to protect CAPPS II from unauthorized access by hackers or other intruders;

“(7) the TSA has adopted policies establishing effective oversight of the use and operation of the system; and

“(8) there are no specific privacy concerns with the technological architecture of the system.

“(b) During the testing phase permitted by paragraph (a) of this section, no information gathered from passengers, foreign or domestic air carriers, or reservation systems may be used to screen aviation passengers, or delay or deny boarding to such passengers.”

Unless the President vetoes this Act (which appears highly unlikely), it will shortly become law. It is thus overwhelmingly probable that, if the Department were to give Congress the 30 days notice required by statute, legislation would take effect within that time substantially limiting the authority of the Department to carry out the proposals in the Notice.

This is exactly the purpose of the 30-day Congressional notice requirement in the statute cited as authority for the Notice: to assure Congress adequate opportunity to consider and enact oversight legislation, before proposed regulations are put into effect.

The Department’s failure to give Congress the notice expressly required by statute, when oversight legislation has already been approved by Congress and awaits only the signature of the President, can scarcely be seen as anything other than a deliberate attempt to frustrate the imminent exercise by Congress of its oversight power.

Accordingly, the Department must advise Congress of these proposals, and must postpone the effective date of the Notice until at least 30 days after Congress is so advised.

In addition, the Department has stated publicly that it desires and intends to include in the system of records created pursuant to this notice, for "test" purposes, "historical data" in existing PNR's and other records. However, the Privacy Act requires that notice be provided prior to the collection of information. As applied to PNR data, this means that the Privacy Act forbids the use of PNR's created prior to the effective date of this Notice, and the provision of notice to the individuals about whom data is to be collected or maintained in the system.

Data in PNR's created prior to the effective date of this Notice thus can only be used in the CAPPS-II or PASSR systems (if at all), to the extent that all the individuals about whom those PNR's contain personally identifiable information (including travellers, travel arrangers, travel agents and airline staff, and others, as discussed earlier in these comments) have received proper actual notice of the use of information about them in these systems, and an opportunity not to provide that information for use in these systems, in accordance with the Privacy Act, after the effective date of this Notice.

PNR's can be created up to 330 days in most cases (and in some cases as much as a year), prior to the intended date of travel, and that in most cases there is insufficient information in a PNR reliably to contact the passenger(s) (much less the other individuals about whom the PNR contains personal information) to provide them with a Privacy Act notice or obtain their consent to provide the information for use in these systems.

The Department must therefore either (A) implement systems to identify the date of creation of each PNR, and use in the CAPPS-II and PASSR systems only information from PNR's created after the effective date of this Notice and the date Privacy Act notices start being provided to all individuals about whom information is entered in PNR's, or (B) use only information in PNR's for flights at least one year after the effective date of this Notice and the date Privacy Act notices start being provided to all individuals about whom information is entered in PNR's.

Finally, in light of the Department's obligation to consider the impact of its proposals on "the public interest in promoting air

transportation”, it should be noted that any sample of “historical” PNR data of any significant size would include PNR data that was originally collected in the European Union, and that is subject to the EU Data Protection Directive and the national laws of EU members implementing the Data Directive.

It is impossible to determine, from any internal evidence in an existing PNR, whether it contains information originally collected in the EU. So any airline, CRS, or travel company that turned over a collection of “historical” PNR data to the Department – even in response to a mandatory order – would inevitably turn over at least some information about EU citizens, originally collected in the EU, which it is forbidden by EU law to turn over without notice and consent of the subject of the data. Even if the transfer of such data were required by USA law, it could result in sanctions for the airline or other travel company including a prohibition on continued operations in the EU. The possible consequences of this for air transportation must be considered by the Department in proposing any such order.

B. The Department has failed to notify those who are asked to supply information what information is being requested, the authority for the solicitation of information, whether providing the information is mandatory or voluntary, and the effects of not providing any part of the requested information, as required by the Privacy Act of 1974.

The Privacy Act of 1974, 5 U.S.C. 552a(e), provides as follows:

“Each agency that maintains a system of record shall – ...

“(3) inform each individual whom it asks to supply information ...

“(A) ... whether disclosure of such information is mandatory or voluntary; ... and

“(D) the effects on him, if any, of not providing all or any part of the requested information”.

The profound vagueness, ambiguity, and contradictions in the Notice and in the Department’s public statements about the proposed systems leave many questions still to be answered as to what the Privacy Act notices for these systems will say.

Among the unanswered questions are the following:

- (1) Who are the “individual[s] whom it asks ... to supply information”?

Will information be requested by the Department from travellers themselves (meaning that they will no longer be able to have reservations made for them by family members, business associates, travelling companions, or other travel arrangers)? Or will information be requested by the Department from travel arrangers, travel agents, or other intermediaries? Or will information be requested by the Department from CRS's and airlines, on the theory that they, and not travellers themselves, are the real owners of information in airline reservations?

The Department hasn't said, and we don't know.

- (2) Is “disclosure of such information ... mandatory or voluntary”, and for whom is it mandatory or voluntary?

Is the obligation to provide information, if any, on the traveller, the person requesting that a reservation be made (travel arranger), the person making the reservation (typically a travel agent, airline staff person, or reservation robot), the entity issuing the ticket (travel agency or airline), or a CRS or airline host system (if so, which one: the booking CRS or airline host system, or the ticketing CRS or airline host system), the airline whose code is on the passenger's ticket for the flight, or the airline actually operating the flight?

And if disclosure of information to the Department is mandatory (for someone), when in the process does it become mandatory? Is it mandatory when a traveller first asks someone (typically a travel arranger or other intermediary) to make reservations for them? When a PNR is created? When a reservation is requested for a specific flight? When a reservation is confirmed? When a ticket is issued? When a reservation is reconfirmed, if it is reconfirmed? When a passenger presents themself for check-in? At the security screening checkpoint? At the gate?

And what information is actually requested or required? The Department seems to assume that these data items are obvious, universal and unambiguous, but they are none of the above:

(A) "full name": Many people change their names, as it is their right to do at any time for any non-fraudulent reason, and many people regularly use different, equally "full", variants of their names.

It is particularly important to note, in this regard, that travellers are not required by the Department or the TSA to produce any documentary evidence of identity in order to travel by air. As a result, ID documents cannot be relied on as a source of information as to travellers names, or as the indication of what is the "full" name.

In this regard, see the e-mail message to Michael Stollenwerk, <majstoll@aol.com>, dated 4/24/2003 6:52:47 PM Eastern Standard Time, from <TSA-ContactCenter@tsa.dot.gov>, cited in the comments of Mr. Stollenwerk and the Fairfax County Privacy Coalition under this docket number (which should be available on the Web, according to the Department's promise, at <<http://www.dhs.gov>>):

"While an air carrier is required to request identification, the actual presentation of identification by the passenger is not absolutely required, and there is currently no prohibition against allowing someone on an aircraft without such identification."

See also the transcript of proceedings before the Honorable Susan Illston, U.S. District Judge, N.D. Ca, Civil 02-3444, January 17, 2003, in *Gilmore v. Ashcroft*, et al., argument of Joseph W. Lobue, Esq., Assistant U.S. Attorney, N.D. Ca, as counsel for the Department and the TSA; transcript at pp. 30-31; available on the Web at <<http://www.freetotravel.org/hearing-011703.html>>:

"The Court: What is the rule ... ?

"Mr. Lobue: ... There is no rule requiring production of ID's for which one can be arrested..."

"The Court: What is the rule, if at all, concerning identification?

"Mr. Lobue: The identification check, every passenger is requested to produce identification." [emphasis added]

(B) "home address": Some travellers have no home, and many have more than one home.

(C) "home phone number": Some travellers have no phone number, or many phone numbers, several or all or any or none of which might be considered a "home" phone number by different definitions.

(D) "date of birth": Some people don't know their date of birth, or have received inconsistent information about it from different sources.

The Department hasn't said, and we don't know.

(3) What are the effects (on whomever) of not providing all or any part of the requested information?

This is the largest of the questions which must be answered in a Privacy Act notice before any information can be collected for these systems. Will providing all or any part of the requested information (and if so, which part) result in refusal to create a PNR? Refusal to accept a request for reservations? Refusal to confirm reservations? Cancellation of reservations? Refusal to sell or to issue tickets? Invalidation of tickets already issued? Denial of transportation? Subjection to more intrusive inspection and search? Detention? Notification or summoning of law enforcement authorities? Other sanction(s)?

The Department hasn't said, and we don't know.

For example, will not providing whatever the Department defines as one's "home phone number", perhaps because one has only a cell phone, result in inability to make reservations, cancellation of existing reservations a specified amount of time before the scheduled flight, subjection to more intrusive screening, or none of the above? It's impossible to determine the answer from anything in the Notice, or that the Department has said to date.

These notices do not, of course, have to be provided in the *Federal Register*. But the Department has not yet provided any copies of such notices, or any evidence that they have been provided to anyone, in spite of my repeated written requests for them, as a journalist, from the Department's public contacts.

Unless and until the Department starts providing notices to all those whom the Department is asking to supply information, answering all of the questions noted above, the Department cannot use any information it does obtain (including PNR's created prior to the date notices answering these questions start being provided) in any system(s) subject to the Privacy Act.

Respectfully submitted,

Edward Hasbrouck

San Francisco, CA, USA
30 September 2003

This document is also available on the Web at:

<[http://hasbrouck.org/articles/
Hasbrouck_DHS_comments-30SEP2003.pdf](http://hasbrouck.org/articles/Hasbrouck_DHS_comments-30SEP2003.pdf)>

Prior preliminary comments (Docket No. DHS/TSA-2003-1):

<[http://hasbrouck.org/articles/
Hasbrouck_TSA_comments-01AUG2003.html](http://hasbrouck.org/articles/Hasbrouck_TSA_comments-01AUG2003.html)>

Comments on the Notice by the Dept. of Transportation for the previous version of this system (Docket No. OST-1996-1437-81), also attached and incorporated as pp. 30-54 of these comments:

<[http://hasbrouck.org/articles/
Hasbrouck_DOT_comments-23FEB2003.pdf](http://hasbrouck.org/articles/Hasbrouck_DOT_comments-23FEB2003.pdf)>

Additional background information and references:

<<http://hasbrouck.org/articles/travelprivacy.html>>
<<http://hasbrouck.org/articles/CAPPS-II.html>>
<<http://hasbrouck.org/articles/PNR.html>>
<<http://hasbrouck.org/cfp2003>>

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 from 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 passenger'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_DHS_comments-30SEP2003.pdf](http://hasbrouck.org/articles/Hasbrouck_DHS_comments-30SEP2003.pdf)>

Prior preliminary comments (Docket No. DHS/TSA-2003-1):

<[http://hasbrouck.org/articles/
Hasbrouck_TSA_comments-01AUG2003.html](http://hasbrouck.org/articles/Hasbrouck_TSA_comments-01AUG2003.html)>

Comments on the Notice by the Dept. of Transportation for the previous version of this system (Docket No. OST-1996-1437-81), also attached and incorporated as pp. 30-54 of these comments:

<[http://hasbrouck.org/articles/
Hasbrouck_DOT_comments-23FEB2003.pdf](http://hasbrouck.org/articles/Hasbrouck_DOT_comments-23FEB2003.pdf)>

Additional background information and references:

<<http://hasbrouck.org/articles/travelprivacy.html>>
<<http://hasbrouck.org/articles/CAPPS-II.html>>
<<http://hasbrouck.org/articles/PNR.html>>
<<http://hasbrouck.org/cfp2003>>