James R. Wheaton, SBN 115230
David A. Greene, SBN 160107
Lowell Chow, SBN 273856
FIRST AMENDMENT PROJECT
California Building
1736 Franklin Street, Ninth Floor
Oakland, CA 94612
Phone: (510) 208-7744
Facsimile: (510) 208-4562
wheaton@thefirstamendment.org
dgreene@thefirstamendment.org
lchow@thefirstamendment.org

Attorneys for Plaintiff Edward Hasbrouck

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

Edward Hasbrouck Plaintiff, vs. U.S. Customs and Border Protection Defendant.	Case No. 3:10-cv-03793-RS **SECOND DECLARATION OF EDWARD HASBROUCK** Date: August 25, 2011 Time: 1:30 PM Courtroom: 3 Judge: The Hon. Richard Seeborg

SECOND DECLARATION OF EDWARD HASBROUCK

I, Edward Hasbrouck, declare as follows:

Reliance on Nonretroactive Application of Privacy Act Exemptions

1. On June 27, 2007, my attorney sent my initial request to CBP for records pertaining to myself from ATS. On August 6, 2007, while that request was pending and before I had received any response, DHS published a Notice of Proposed Rulemaking (NPRM) at 72 Federal Register 43567-43569, by which it proposed to exempt ATS records from certain requirements of the Privacy Act, and solicited comments from the public on that proposal. On September 5, 2007, I submitted comments on behalf of the Identity Project objecting to the exemptions proposed in the NPRM.

2. As of the date of the NPRM proposing to exempt ATS from some of the provisions of the Privacy Act, what would later be renamed BCI was part of ATS. No SORN giving notice of the existence of BCI as a separate system of records was published until July 25, 2008, at 73 Federal Register 43457-43459. Exhibit F to my declaration of June 21, 2011, consists of the comments I submitted on behalf of the Identity Project objecting to that SORN and to the operation of the BCI system of records as illegal.

3. No final rule was issued pertaining to exemption of ATS or BCI from any provisions of the Privacy Act until February 3, 2010. Laurence Castelli was listed as contact for each of these SORNs, NPRMs, and final rules.

4. To the best of my knowledge, no proposal had been made to exempt ATS records from any of the provisions of the Privacy Act at the time I made my initial 2007 request for those records. To the best of my knowledge, no rule exempting ATS from any of the provisions of the Privacy Act had been finalized at the time of my 2007 appeal or at the time of any of my 2009 requests or appeals. On the contrary, I knew that DHS had solicited comments on the proposed exemptions, had received comments including my own objecting to the proposed rule, and was required by the Administrative Procedure Act to consider them before it could finalize any such rule. Until the issuance of the final exemption rules for ATS and BCI on February 3, 2010, I assumed that those comments were under review by DHS, and specifically by Mr. Castelli.

5. I regularly checked both the Code of Federal Regulations and the Federal Register for any final rules exempting these systems of records from any of the provisions of the Privacy Act. In particular, I checked for the existence of any such rules before making arrangements for each of my international trips.

6. In deciding whether to travel internationally, and in making travel arrangements including airline reservations, I relied on the protections of the Privacy Act. I knew that PNR and other data pertaining to me entered in PNRs, API data, and other business records by airlines, travel agencies, or other travel companies, and obtained from them by CBP, or generated by or compiled from other sources by CBP, would be contained in systems of records subject to the provisions of the Privacy Act. I knew that I would be entitled, on request, to access to records pertaining to me from the ATS and BCI systems of records, to an accounting of all disclosures from those systems of records, and to correct inaccurate or irrelevant records. I relied on the knowledge that DHS was required to consider comments such as my own and promulgate final rules before it could exempt these systems of records from these requirements.

7. If I had known or believed that DHS could later promulgate rules retroactively exempting itself from the requirement to comply with pending Privacy Act requests or appeals, I would have acted differently in making arrangements for international travel, I would have been less patient with CBP's delays in responding to my requests, and I would have filed this lawsuit years earlier.

8. In particular, if I had known that DHS could issue such Privacy Act exemption rules applicable to pending Privacy Act requests or appeals, I would have taken steps to ensure that less information was entered into PNRs pertaining to me. Since I would not have had the assurance of being able to access PNR data pertaining to me from DHS, or to obtain an accounting of disclosures of that data, I would have chosen to make my reservations through travel companies based in other countries whose privacy and data protection laws would have entitled me to obtain that information from those travel companies (even if I could not do so from DHS), rather than through travel companies in the USA that are subject to no privacy or data protection laws, and which have no obligation to disclose PNRs or other business data to

travelers or to maintain or provide any record or accounting of disclosures of such data to third parties. If I made reservations through a travel agency in the USA, they (as a commercial entity in the USA) don't have to tell me what they have said about me in PNRs. Travel agents or airlines in some other countries with better privacy regimes for commercial data, including Canada and the European Union, do have to tell me (if I ask) what information they put in my PNRs. The existence or non-existence of Privacy Act exemptions for these systems of records including data derived from commercial travel records would have been a significant factor in my choices of travel agencies.

9. If I had been aware of Privacy Act exemptions in effect for these systems of records, but had nonetheless dealt with travel companies in the USA, rather than those in foreign jurisdictions with stronger rights of access to personal data about me, I would have sought to negotiate contractual commitments from those U.S. travel companies, or would have chosen companies with contractually binding privacy policies, that would allow me to control what data was entered in PNRs pertaining to me, to access that data, and to obtain an accounting of all disclosures of that data to third parties including CBP.

10. From my experience as a travel agent working in travel agencies that specialized in importing and exporting tickets internationally and having tickets issued by agents in other countries, I would have been able, if I had known that it was necessary in order to safeguard my privacy rights, to make all of my airline reservations including reservations for travel within the USA through travel agencies or other intermediaries in other countries such as Canada or the European Union where I would have been assured of such rights of access to information pertaining to me under those countries' laws. Had I known that DHS could issue rules retroactively exempting itself from the requirements of the Privacy Act in effect at the time requests and appeals were made, I would have made the extra effort to make my reservations through agencies in such countries.

11. My choices of travel services providers and intermediaries were deliberate, carefully considered, based on the best available information about the status of CBP's rules and the Privacy Act, and made in reliance on that information including in particular the status of

DHS's rulemakings with respect to Privacy Act exemptions and the status of my then-pending requests and appeals. I would be irreparably harmed by being retroactively denied the opportunity to make different choices on the basis of the exemption rules later promulgated by DHS.

Passenger Name Records

12. As discussed in more detail in my FAQ, "What's In A PNR?," available at http://hasbrouck.org/articles/PNR.html, a passenger name record (PNR) is a business record in the database of a travel company containing information about a set of reservations for one or more people traveling on the same itinerary. A single PNR can contain information about multiple people traveling together, multiple travel services (flights, hotels, etc.), and data entered by staff of multiple companies, including the travel agency and any of the providers of travel services included in the PNR. A PNR pertaining to an individual is created or added to when a travel agency, tour operator, or other travel company makes reservations for any of those services, either at the request of the individual or at the request of an intermediary such as a traveling companion, business associate, group coordinator or travel manager, or another travel company (for example, when an airline ticket wholesaler or "consolidator" makes reservations at the request of a retail travel agent). An individual may not even know that a reservation in which they are mentioned has been created, or by whom. Travelers rarely see PNRs pertaining to them, rarely enter data directly in PNRs, and rarely know or can control what data is included in PNRs pertaining to them. There is typically a chain of intermediaries between the traveler and the person entering the data in the PNR. Most travel agencies and airlines outsource the hosting of their PNR databases to computerized reservation systems (CRSs), but if the travel agency requesting the reservation subscribes to a different CRS that the one which hosts the airline's PNRs, the message will have to be transmitted between those CRSs. If a reservation is created on a travel website, the data entered in the PNR is typically generated by multiple software layers and interfaces including web server software and scripts, booking engine software, a CRS application programming interface (API) or terminal emulator, CRS connectivity and messaging layers, and other middleware.

13. Although the Security Directives from DHS to airlines are secret, no publicly

disclosed statute or regulation requires any airline to structure its data in the form of PNRs, imposes any requirements on what data must be included in PNRs or how it must be formatted, or imposes any limits or restrictions on what data may or may not be included. The global travel industry PNR data architecture is designed to permit a travel agency, tour operator, or other travel company to store complete information about a multi-component itinerary in a single PNR, including information about flights on multiple, possibly unrelated airlines, hotel and car rental reservations, and other travel services provided by different (and perhaps competing) suppliers. PNRs are business records of airlines, travel agencies, CRSs, and other travel companies, and are used for a wide range of purposes including transaction processing, customer profiling, and customer relationship management. Staff of each of these companies participating in a PNR have the ability to enter data and send messages which will be stored in the PNR. These companies can, and do, include in PNRs whatever information they find commercially useful. Some of these entries and messages are generated automatically by scripts and message and transaction processing systems, while others are entered manually. While the formats in which PNR data are stored vary, the systems in which they are stored are designed for global real-time accessibility and interoperability, and there are well-developed global industry standards such as the "ATA-IATA Reservations Interline Message Procedures - Passenger" (AIRIMP) protocol to ensure the ability of different companies using different CRSs or PNR hosting systems to exchange messages and data to be included in PNRs. Tens of thousands of travel agencies, airline offices, and offices of other travel companies around the world, and a million or more individual employees and contractors of these companies, have access through CRSs or otherwise to PNR databases and the ability to enter data in PNRs. PNRs thus can, and do, contain an unlimited quantity and variety of data originating with numerous third parties around the world, some of it in the form of unstructured free text. CBP requires that, in all cases where a PNR contains a flight between a point in the U.S. and a foreign point, or overflying U.S. airspace, the *entirety* of the PNR—including the free-text general remarks and whatever other data has been entered by anyone with access to the PNR—must be made available to CBP for import into ATS.

14. PNRs can contain information about aspects of a journey other than air

transportation, such as hotel reservations and other travel services, even in what are considered in travel industry jargon to be "air-only" PNRs. Information about these other travel services can be included in the "OSI" (Other System Information), and "SSR" (Special Service Request) elements of the PNR. For example, in reviewing records from ATS released to another requester by CBP, I have seen a PNR for two people, for whom the airline had reserved a hotel for an involuntary overnight layover, which included an SSR entry with a code showing whether a room with one bed or two had been requested for those two travelers. This is a normal and expected example of standard travel industry practices.

15. The SORNs for ATS specifically mention OSI, SSR, and "General Remarks" among the "Categories of Information in the [ATS] System" and among the types of data derived from PNRs and included in ATS. "OSI" entries can be used by travel agency or airline staff with access to PNRs to enter, and to send to airlines, arbitrary free-text messages. "Remarks" in PNRs are intended to be used for an unlimited range of free-text data entry. This information can—and in some cases does—include remarks about the personal foibles of the traveler (to assist other travel agency or airline staff in dealing with the traveler), and/or derogatory descriptions of interactions with customer service staff. Travelers do not normally see the PNRs that contain information pertaining to them, and do not know or control what information has been entered about them.

16. In the absence of a valid exemption from the requirements of the Privacy Act, travelers can rely on the Privacy Act for access to CBP records of PNR data pertaining to them (even data they were unaware had been entered into PNRs), an accounting of disclosures of those records, correction of inaccurate records, and expungement of irrelevant records. Travelers can make informed choices about what to do if those rights are terminated—such as "self-help" measures to minimize the PNR data provided to CBP by making reservations for hotels, car rentals, etc. separately from airline reservations, or negotiating contractual rights to access to and/or control of what information in entered in PNRs by travel companies—only if they receive notice before such exemptions take effect.

//

Travel Agent Expertise and Knowledge of Travel Industry Procedures

17. Defendant CBP cites a decision of another court which distinguished ATS data from PNR data as it is stored in Computerized Reservation Systems (CRSs) by travel companies, and found that "Mr. Hasbrouck's affidavit is based on the faulty assumption that these systems are the same." Defendant's declarations in this case appear to make the same assumption that they criticize as faulty: They assume, on the basis of their knowledge of ATS records, that they understand the nature of the data imported into ATS from CRSs, and the business process by which that data is entered into those PNRs before being transferred to CBP.

18. As an expert in travel industry business processes with respect to PNRs, including practices with respect to the entry of data in PNRs, I can find no evidence whatsoever in the declarations of Ms. Suzuki or Mr. Castelli that they have any experience, knowledge, or basis of expertise whatsoever in travel industry practices with respect to what data is entered in PNRs, how, by whom, and through what chain of intermediaries.

19. Mr. Castelli bases his belief that no search for misspelled names was necessary on the mistaken belief that, at paragraph 10 of his supplemental declaration, "Because the PNR records in ATS-P consistent information is supplied either directly by the traveler or at his/her direction (*i.e.*, through a travel agent), it is unlikely that the Plaintiff would misspell his own name."

20. No expert in travel agency procedures could possibly believe that ATS data consisting of PNR data imported from airlines or the CRSs that host airline PNRs consists solely of information supplied directly by the traveler or at his/her direction. Any such expert would be aware that misspellings of names in PNRs is not only common but can derive from numerous normal events in the chain of transmission of information between intermediaries, and are not limited to cases in which people misspell their own names.

21. It is not necessary for me to know anything about how ATS stores PNR data to know that, unless ATS include some magic module for correcting misspellings, misspelling of names in PNRs will result in misspellings of names in ATS. Knowledge of the ways that names can come to be misspelled in PNRs is sufficient to understand the potential for names to be

misspelled in ATS records consisting of PNRs.

22. DHS first gave public notice of the existence of ATS as a system of records subject to the Privacy Act through a SORN published on November 2, 2006, at 71 Federal Register 64543-64546, and a supplemental notice published on December 8, 2006 at 71 Federal Register 71182. I submitted comments on behalf of the Identity Project in response to each of these notices.

23. In those comments submitted to DHS, I itemized some of the categories of individuals other than travelers about whom PNRs and thus ATS might contain information, and some of the intermediaries through whom information typically passes (with the possibility of errors in spelling or transcription at each stage) between the traveler and the person who actually enters data in the PNR. Those comments discussed, in detail, the factual error in the DHS notices about ATS—the same error repeated in Mr. Castelli's declaration in this case—in their erroneous claim that all PNR data is supplied or entered by travelers themselves.

24. As I explained in those comments, which DHS had a duty to review as part of the rulemaking, and with which they are thus presumably familiar, "Only in the case of airline staff making reservations for their own travel is any information entered directly into a PNR by the data subject. Information in a typical PNR comes from multiple sources including third parties other than the airline and the passengers. And the information provided by passengers is typically provided through at least one, typically two or three, and sometimes half a dozen intermediaries, many of them unknown to the passenger . . . ."

25. Even as a travel agent making reservations for my own travel, I did not enter data directly in my own PNRs in the airline host systems from which they were obtained by CBP. I entered data in the CRSs used by the travel agencies where I worked. Typically, the CRS in which I entered the data would then send a message (invisible to me) to the CRS or other system which hosted the airline's PNRs, which would result in the creation of a separate PNR in that host system. Because the inter-CRS and inter-airline "AIRIMP" message protocol does not require redundancy, error-checking, or message acknowledgment, errors in message receipt are a routine occurrence. While most AIRIMP messages are received correctly, message failures and

errors are sufficiently common that standard travel agency and airline staff training in CRS usage and reservation procedures includes training in how to deal with these failures and errors.

26. Some of my airline reservations have been made by traveling companions or by clients or business associates (or by their travel agents) who may have been much more likely than me to misspell my name. In other cases, even when I was initiating a request for reservations myself as a travel agent, the PNR was not created by me but by a wholesale airline ticket "consolidator" who I or someone else at the travel agency where I worked contacted to make reservations on my behalf, in order to take advantage of the lower price offered by such a consolidator. These communications from traveler to travel agent or travel arranger (for example, from me to a consulting client or to the sponsor of an event at which I had been invited to speak), and from the retail travel agent or agency (in some cases, myself) to the wholesale consolidator, sometimes occur by telephone or fax, necessitating retyping of passenger names and the possibility of transcription errors. Even when reservation requests are transmitted by e-mail, technical and business reasons (such as receipt of the e-mail message on a different workstation than the one with access to the CRS) often lead to retyping of names when the actual PNRs are created based on those messages, with the inevitable risk that errors in spelling will be introduced in retyping. Even "cutting and pasting" from an e-mail message to a PNR entry on the same workstation can inadvertently introduce errors, such as truncating a name by a letter due to a slight mouse or keyboard error in selecting the text to be copied.

27. Because I worked at travel agencies that specialized in international consolidator tickets for travel around the world, it was especially common in my own case for those reservations to be made by consolidators in other countries, who were not native speakers of English, and to whom my name may have seemed even more unusual and difficult to spell than it might be for the typical person in the USA.

Identifiers in PNRs

28. Standard business practice in the travel industry in many countries has been not to include first or middle names in PNRs, but only a first initial. Travel agencies where I worked constantly had to explain to our customers, when reservations had been made and tickets issued

with only a last name and first initial by overseas consolidators, that this was normal and not a cause for alarm. No airline or travel industry business protocol requires full first or given names in PNRs or on tickets. Full names are included in PNRs and on tickets in many parts of the world only when specially requested and/or required by governments. I have traveled using tickets based on PNRs in which only my first initial, and not my full first name or any middle name or initial, were entered.

29. Mr. Castelli states in paragraph 10 of his supplemental declaration that, "because each PNR record was manually reviewed for relevancy any variation on the spelling of the Plaintiff's last name would have been examined." However, it is obvious to anyone familiar with PNR data entry protocols that this is factually false. Mr. Castelli claims in paragraph 9 of his supplemental declaration that every PNR in the ATS-P database that contained the term "Edward" was reviewed. Given that the ATS database contains millions of PNRs, and the commonness of the name "Edward," this claim does not seem credible. At least tens of thousands of PNRs in this database must have contained the name "Edward," and reviewing them all would not have been feasible. But even if such a review was actually conducted, it would not have identified any PNRs in which my first name was entered only as an initial "E." Since a large proportion of PNRs routinely have included only a first initial, and not a first name, a search based on full first name is not reasonably calculated to retrieve all responsive records.

30. Some PNRs identifiable with an individual do not contain that individual's name at all. These include PNRs identifiable with an individual through the presence of some personal identifier other than a name, including but not limited to:

a. PNRs paid for using the credit card of someone other than one of the travelers named in the PNR, identifiable with the payer by their credit card number as a personal identifier;

b. PNRs for travel by other people, identifiable with an individual through the inclusion of that individual's telephone number (as a contact phone number, a reconfirmation phone number, a phone number associated with an address for ticket delivery, a phone

number for a next-of-kin or other emergency contact, etc.); and

c. Split PNRs (that is, PNRs that result when a PNR initially created for two or more travelers is split into two or more individual PNRs as a result of diverging itineraries) for other travelers associated with an individual by a reference in the PNR and its "history" (change log) portion to the PNR having been "split" or "divided" from an original PNR including an additional traveler or travelers, and by a cross-reference to the record locator of the other PNR.

31. Only by knowing by what personal identifiers records are retrieved from these CBP systems of records can an individual know what personal identifiers to provide to CBP in a request for records, in order to effectively exercise their right to access records pertaining to them. In requesting this information from CBP, I was requesting information required to be included in the SORN for each such system, in order to use it to exercise my right to access records pertaining to me. I believe that my purpose in requesting this information is exactly the purpose for which this information is required to be included in the published SORN.

32. Ms. Suzuki says in paragraph 8 of her supplemental declaration that, "Based on my experience a search using the first name, last name and date of birth is most likely to retrieve all responsive records about an individual." However, she gives no indication as to how she would know if a search had not retrieved all responsive records.

33. In my capacity as a consultant to the Identity Project, I have been contacted by numerous people who have requested their PNR and other ATS records from CBP. Many of those people have told me that they have never received any response to their request. Many of those who did receive some response have told me that they believe CBP's response to be incomplete because it does not include records of international trips to and from the USA that they know they took.

34. Ms. Suzuki has no access to the people—primarily staff of travel agencies, tour operators, cruise lines, and airlines—who enter data in PNRs or the software used to relay PNR data, no way to question these people or investigate how or why particular records haven't been

found, and no business necessity to find out how particular PNR data came to be incorrect or was not found.

35. In contrast, in a business context erroneous or missing data in a customer's PNR is a customer service and/or liability issue. Understanding, avoiding, and dealing with these problems is a business necessity. As the person often responsible at the travel agencies where I worked for this sort of business forensics, I was able to review the underlying data sources and the chain of communications and speak directly with the people who had been involved in making the reservations. From that experience, I know that misspellings of names are a common reason why an initial search for a reservation is unsuccessful, and would be an even more common source of such problems if all major CRSs did not rely by default on phonetic similar name matching rather than solely on exact name search.

Documents Believed to Exist but That Have Not Been Provided

36. Ms. Suzuki says in paragraph 6 of her supplemental declaration that "Plaintiff has not articulated which specific records he believes exists that CBP has not provided to him." As was articulated in my earlier appeals, pleadings, and declaration, I believe that the responsive records which exist but which CBP has not provided to me include (but are not limited to) the following:

a. FOIA request docket or log entries;

b. FOIA appeal docket or log entries;

c. Privacy Act request docket or log entries;

d. Privacy Act appeal docket or log entries;

e. Workflow and status records such as records showing when and to which employee or office requests and appeals were assigned;

f. System-level electronic logs from ATS and other systems showing when and by what user ID which records pertaining to me were retrieved in response to my requests or appeals or otherwise;

g. System-level electronic records of the "Sharepoint" document management system used by DHS and component FOIA and

Privacy Offices, as described in DHS Congressional testimony;

h. Records of the CBP Office of Intelligence and Operations Coordination (OIOC) including e-mail messages;

i. Records of the CBP Privacy Branch including e-mail messages;

j. Records of the CBP FOIA Branch including e-mail messages;

k. Records of the CBP Office of Field Operations (OFO) including e-mail messages;

l. Records of any other offices with which those offices communicated concerning these requests and appeals, including e-mail messages;

m. Risk assessments;

n. Rules used in determining risk assessments;

o. Records maintained in order to comply with requirements to be able to provide an accounting of disclosures;

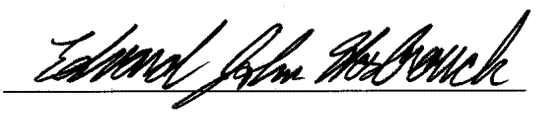
p. Information required to be included in SORNs, showing by which personal identifiers records from these systems can be retrieved, including information contained in software specifications, procurement contracts, and documentation, and in records of offices developing or supervising software development or contractors;

q. Records of my original, signed and dated 2007 requests and appeals (which could not and would not have been responded to initially if they weren't signed to authorize release of records), and records of the office(s) or individual(s) to which or to whom they were assigned; and

r. Some record of who Stephen Christensen, the person who signed for my appeal letter, is and in what capacity he worked for CBP.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed in the city and county of San Francisco, California, on 28 July 2011.



By: Edward John Hasbrouck