

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

7 Attorneys for Plaintiff Edward Hasbrouck

8 UNITED STATES DISTRICT COURT  
9 FOR THE NORTHERN DISTRICT OF CALIFORNIA

10 Edward Hasbrouck  
11 Plaintiff,  
12 vs.  
13 U.S. Customs and Border Protection  
14 Defendant.

Case No. 3:10-cv-03793-RS

**[PROPOSED] ORDER ON PARTIES'  
CROSS-MOTIONS FOR SUMMARY  
JUDGMENT**

Date: August 25, 2011

Time: 1:30 PM

Judge: The Hon. Richard Seeborg

17 **PROPOSED ORDER**

18 This action arises from the several Privacy Act and Freedom of Information Act (FOIA)  
19 requests filed by Plaintiff Edward Hasbrouck. The Privacy Act requests were directed at obtaining  
20 documents and records responsive to: (1) Hasbrouck’s 2007 request for records relating to or  
21 identifiable with him in Defendant Customs and Border Protection (CBP)’s Automated Targeting  
22 System (ATS) system of records; (2) Hasbrouck’s 2009 request for records relating to or identifiable  
23 with him in the ATS, Advance Passenger Information System (APIS), Border Crossing Information  
24 System (BCIS), and Customs and Border Protection TECS systems of records; and (3) Hasbrouck’s  
25 2009 request for records created by CBP or other agencies in the course of processing his 2007  
26 Privacy Act request and subsequent appeal. The FOIA requests were directed at obtaining documents  
27 and records responsive to: (1) Hasbrouck’s 2009 request for records created by CBP or other  
28 agencies in the course of processing his 2007 Privacy Act request and subsequent appeal, and (2)

1 Hasbrouck's 2009 request for documents and records describing the search systems and methods,  
2 indexing, query formats and options, data fields and formatting, and the numbers or other identifying  
3 particulars by which Passenger Name Record (PNR) or other data can be retrieved from the various  
4 CBP systems of records.

5 The parties have brought cross-motions for summary judgment on the issues of (1) whether  
6 CBP has violated its duties under the Privacy Act by improperly withholding records from the ATS  
7 and BCIS records systems and did not produce any accounting of disclosures of such records; (2)  
8 whether CBP violated its duties under FOIA because it failed to segregate nonexempt material and  
9 because it withheld material that was not exempt under exemption 7(E) failing to adequately search  
10 for the records Hasbrouck requested; and (3) whether CBP violated both the Privacy Act and FOIA  
11 by conducting inadequate searches for records responsive to Hasbrouck's requests.

12 The cross-motions having come before this Court for hearing on August 25, 2011, the Court  
13 GRANTS Plaintiff's cross-motion for summary judgment and DENIES Defendant's motion for  
14 summary judgment. The Court hereby ORDERS as follows:

15 **I. THE PRIVACY ACT**

16 The Court finds that CBP has not complied with the Privacy Act. The Privacy Act regulates  
17 the collection, maintenance, disclosure of, and access to an individual's personal information  
18 maintained by federal agencies. 5 U.S.C. § 552a. Except when an agency has properly promulgated  
19 an exemption, an individual is entitled to access records and information pertaining to him, and to  
20 accountings of disclosures made to others. 5 U.S.C. §§ 552a(c), (d), (j), (k).

21 CBP has treated much of the ATS and the entire BCIS as exempt from that law's disclosure  
22 and accounting requirements and accordingly has withheld such records. However, no valid  
23 exemption for these records was in place at the time Hasbrouck made his requests for these records.

24 **A. CBP's statements in its SORNS that ATS records are exempt are not**  
25 **"enforceable rules"**

26 An agency may issue rules exempting its systems of records from the Privacy Act's access  
27 provisions. 5 U.S.C. §§ 552a(j), (k). However, an agency, in issuing such rules, must strictly comply  
28 with certain provisions of the Administrative Procedures Act (APA), 5 U.S.C. § 553. 5 U.S.C. §

1 552a(j)(2), (k)(2); Louis v. Dep't of Labor, 419 F.3d 970, 974-76 (9th Cir. 2005).

2 The APA requires that for a rule to be valid, the agency must complete three tasks. First, the  
3 agency must publish a notice of proposed rulemaking. 5 U.S.C. § 553(b). Second, the agency must  
4 accept public comment. Id. § 553(c). Third, and only after this public comment period has expired,  
5 can the agency issue a “final rule” making the exemption effective. Id.; Louis, 419 F.3d at 975.

6 A system of records notice (SORN) can never simultaneously serve both as a notice of  
7 proposed rulemaking and a final rule. The APA requires that an agency issue a separate “final rule”  
8 only after the notice and proposed rulemaking processes are complete. 5 U.S.C. § 553(c)

9 CBP here improperly relies on the SORN for ATS in lieu of a proper rulemaking. [Def.'s  
10 Mot. Summ. J. 7-8; Suzuki Decl. ¶ 19 & n.9 & Exh. O] The SORN for ATS does not meet the  
11 requirements for a rulemaking as required by the Privacy Act and the APA. The SORN for ATS  
12 merely states that the ATS records “are exempt.” 72 Fed. Reg. 43650, 43656 (Aug. 6, 2007). CBP  
13 cannot exempt ATS on the basis of the system's SORN.

14 **B. CBP cannot rely on the ATS or BCIS exemption because the final rules**  
15 **implementing the exemptions were not effective until 2010**

16 A “final rule” setting forth the exemption was not in place until February 2010. See 6 C.F.R.  
17 pt. 5, app'x C, ¶ 45 (2011); 75 Fed. Reg. 5487, 5487 (Feb. 3, 2010). Applying the 2010 rule to  
18 Hasbrouck's 2007 and 2009 Privacy Act requests would have impermissible retroactive effect. See  
19 Landgraf v. USI Film Prods., 511 U.S. 244, 265 (1994); Mejia v. Gonzales, 499 F.3d 911, 977 (9th  
20 Cir. 2007). CBP cannot rely on the ATS exemption to withhold from Hasbrouck risk assessments  
21 and accountings of disclosures.

22 Similarly, BCIS is not exempt under the Privacy Act with respect to Hasbrouck's 2009  
23 request for BCIS data because the final rule exempting the system was not final until 2010. See 6  
24 C.F.R. pt. 5, app'x C, ¶ 46 (2011); 75 Fed. Reg. 5491, 5491 (Feb. 3, 2010).

25 Accordingly, with respect to the Privacy Act, Defendant is hereby ORDERED:

26 A. From the ATS system of records, to release records responsive to  
27 Hasbrouck's June 27, 2007 and October 15, 2009 Privacy Act requests  
28 relating to risk assessments and accountings of disclosures that were withheld

1 from him.

- 2 B. From the BCIS system of records, to reprocess Hasbrouck's October 15, 2009  
3 Privacy Act request as a Privacy Act request without consideration of any  
4 exemption and release all records responsive to the request.

5 **II. FOIA**

6 The Court further finds that CBP did not comply with FOIA. Hasbrouck challenges CBP's  
7 withholding the entirety of the ATS and TECS user guides under Exemption (7)(E). CBP has failed  
8 to justify withholding these documents in full.

9 FOIA exemption (7)(E) protects from disclosure only those law enforcement records that  
10 "would disclose techniques and procedures for law enforcement investigations or prosecutions, or  
11 would disclose guidelines for law enforcement investigations or prosecutions if such disclosure  
12 could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E).

13 **A. CBP did not fulfill its duty to segregate nonexempt material**

14 To justify a claim that segregation is impossible, an agency must supply a "relatively detailed  
15 justification, specifically identifying the reasons why a particular exemption is relevant and  
16 correlating those claims with the particular part of a withheld document to which they apply." King  
17 v. Dep't of Justice, 830 F.2d 210, 224 (D.C. Cir. 1987). See also Armstrong v. Exec. Office of the  
18 President, 97 F.3d 575, 578 (D.C. Cir. 1996). The government's justifications must not be  
19 conclusory; a blanket statement that exempt and nonexempt portions of a record are so intertwined  
20 as to prevent disclosure is insufficient to justify nonsegregability. Pac. Fishers, Inc. v. United States,  
21 539 F.3d 1143, 1148 (9th Cir. 2008); Defenders of Wildlife v. U.S. Border Patrol, 623 F. Supp. 2d  
22 83, 90 (D.D.C. 2009). The agency must also describe "what proportion of the information in a  
23 document is non-exempt and how that material is dispersed throughout the document." Nat'l Res.  
24 Def. Council v. Dep't of Educ., 388 F. Supp. 2d 1086, 1097 (C.D. Cal. 2005).

25 CBP's conclusory explanation that nonexempt information in nonsegregable does not provide  
26 the required specific, detailed justification. CBP's explanation merely recites the general rule that  
27 nonexempt material that is "inextricably intertwined with the exempt information" need not be  
28 segregated and disposed. [Suzuki Decl. ¶ 42] CBP has not carried its burden of justifying

1 nonsegregability.

2 **B. Exemption (7)(E) does not apply to all of the information in the user guides**

3 **1. Instructions required to be made public under the Privacy Act**

4 The Privacy Act requires that agencies publish in the Federal Register “the policies and  
5 practices of the agency regarding storage, retrievability, access controls, retention, and disposal of  
6 the records” in a system of records. 5 U.S.C. § 552a(e)(4)(E). This information cannot be exempted  
7 under FOIA, even if the agency neglected its duties under the Privacy Act and failed to publish the  
8 information. See Doe v. Gen. Servs. Admin., 544 F. Supp. 530, 536-37 (D. Md. 1982).

9 CBP’s description of the exempted information appears to include the type of information  
10 that should have been published in the SORN for each records system. The user guides apparently  
11 contain “instructions on how to retrieve records.” [Suzuki Decl. ¶ 40] This information fits squarely  
12 within the Privacy Act’s command that “policies and practices of the agency regarding storage,  
13 retrievability, access controls” be disclosed.

14 **2. Routine techniques and procedures and instructions to staff**

15 Exemption (7)(E) does not apply unless CBP demonstrates how release of the withheld  
16 material would improperly reveal actual law enforcement techniques or procedures. First, exemption  
17 (7)(E) does not apply to techniques or procedures that are obvious, routine or generally known to the  
18 public. Rosenfeld v. Dep’t of Justice, 57 F.3d 803, 815 (9th Cir. 1995); Albuquerque Publ’g Co. v.  
19 Dep’t of Justice, 726 F. Supp. 851, 858 (D.D.C. 1989). An agency cannot refuse to disclose a  
20 technique because although the general use of the technique is known, a specific application of that  
21 technique is not known. Rosenfeld, 57 F.3d at 815. Second, exemption (7)(E) does not apply to  
22 records that fall within the scope of 5 U.S.C. § 552(a)(2), which provides that an agency “shall make  
23 available . . . (C) administrative staff manuals and instructions to staff that affect a member of the  
24 public.” Firestone Tire & Rubber Co. v. Coleman, 432 F. Supp. 1359, 1366 (N.D. Ohio 1976).

25 CBP’s justification for why disclosure of the ATS and TECS user guides would reveal  
26 techniques and procedures suggests that at least some of the techniques or procedures are actually  
27 routine and well known to the public. Moreover, portions of the ATS and TECS user guides appear  
28 to relate to matters that are usually found in administrative staff manuals and instructions to staff.

1 Exemption (7)(E) is being asserted in this case to protect two general categories of  
2 information: (1) information that would reveal procedures for processing international travelers; and  
3 (2) information that would reveal how to navigate sensitive law enforcement databases. [Suzuki  
4 Decl. ¶ 38] The information in the user guides were withheld as part of the second category, that is,  
5 they allegedly “provide a road map of how to use the law enforcement databases.” [Suzuki Decl.  
6 ¶ 40] As Hasbrouck is only challenging the claim of exemption with respect to the user guides, this  
7 second category of information is the only one at issue.

8 With respect to this navigational information, unless CBP has devised some especially  
9 labyrinthine navigational scheme as an added layer of security against hackers, this withheld  
10 information is likely to be the type of routine, instructional material to which the exemption does not  
11 apply. How to use drop-down menus, perform searches and read search results are well known to  
12 anyone who has used computer software with database capabilities.

13 Any withheld information that describes such routine navigational techniques is not exempt  
14 under exemption (7)(E) and must be disclosed.

15 **3. Information that cannot reasonably be expected to risk circumvention**  
16 **of the law**

17 To meet its burden on exemption 7(E), the government must show “that the records reveal  
18 law enforcement techniques or guidelines that, if disclosed, could reasonably be expected to risk  
19 circumvention of the law.” Council on Am. Islamic Relations v. FBI (CAIR), 749 F. Supp. 2d 1104,  
20 1123 (S.D. Cal. 2010) (internal quotation marks omitted). CBP must demonstrate a circumvention  
21 risk regardless of whether the information is a “technique or procedure” or a “guideline.” See CAIR,  
22 749 F. Supp. 2d at 1123; Gordon v. FBI, 388 F. Supp. 2d 1028, 1035 (N.D. Cal. 2005); Feshbach  
23 v. SEC, 5 F. Supp. 2d 774, 786 & n.11 (N.D. Cal. 1997). Accord Catledge v. Mueller, 323 F. App’x  
24 464, 466-67 (7th Cir. 2009); Davin v. Dep’t of Justice, 60 F.3d 1043, 1064 (3rd Cir. 1995).

25 CBP fails to show how only complete withholding of the ATS and TECS user guides will  
26 prevent circumvention of the law. Courts must not simply defer to the government’s claims that  
27 disclosure would facilitate circumvention of the law. Rather, specific, nonconclusory explanations  
28 of how disclosure would enable individuals to evade the law are required. See El Badrawi v. Dep’t

1 of Homeland Security, 583 F. Supp. 2d 285, 312-13 (D. Conn 2008). A conclusion, without  
2 explanatory detail, that disclosure “would reveal internal procedures, techniques, and strategies and  
3 allow broker-dealers to frustrate or deceive the staff in its efforts to enforce compliance with federal  
4 security laws,” for example, is insufficient. Feshbach, 5 F. Supp. 2d at 786. This is true even when  
5 the withheld records involve matters of national security. See, e.g., Gordon, 388 F. Supp. 2d at 1036-  
6 37.

7 With respect to information specifically regarding the navigation of a database, an agency  
8 must provide a specific explanation of how “disclosure of a system’s architecture (i.e., where certain  
9 pieces of information are stored in relation to others) could allow persons to circumvent” the  
10 database and its purpose. See ACLU of Wash. v. Dep’t of Justice, 2011 WL 887731, at \*8 (W.D.  
11 Wash. 2011). If withheld material “simply reveal[s] the location of information within” an agency’s  
12 databases and systems, the agency fails to justify nondisclosure if its explanation does not make clear  
13 how the information relates to the agency’s concerns. Id.

14 Although CBP has asserted a risk of circumvention, it has not explained why disclosure  
15 presents such a risk. CBP states that the user guides include “step-by-step” instructions on how to  
16 retrieve, query and navigate the database. [Suzuki Decl. ¶ 40] A risk of circumvention exists, then,  
17 only if one presumes that others have unauthorized access to the database. The secrets CBP wants  
18 to protect are not the instructions for how to find information in the database, but the information  
19 itself. There may indeed be some component of these user guides that deals with some specific  
20 substance of the ATS and TECS programs that is not generally known and the effectiveness of which  
21 depends on such substance not being known. But CBP has not explained that that is the case.

22 CBP has not carried its burden of justifying its claims of exemption 7(E).

23 Accordingly, with respect to FOIA, Defendant is hereby ORDERED:

- 24 A. For all material withheld under Exemption (7)(E) contained in the documents  
25 described in Defendant’s Vaughn Index as pages 000017-187, to segregate  
26 and release all step-by-step instructions on how to navigate a law  
27 enforcement database, step-by-step instructions on how to retrieve records  
28 from a law enforcement database, specific drop down menus and instructions

1 for querying and navigating the database, names of specific modules within  
2 a law enforcement database, computer query codes, precise details of query  
3 screens, query screen field descriptions, navigation buttons, instructions on  
4 how to read results screens, system capabilities with respect to records, and  
5 information about querying abilities and results, which are nonexempt  
6 (1) because they describe policies and practices of CBP regarding storage,  
7 retrievability, and access controls, (2) because they describe routine and well-  
8 known navigational techniques or administrative matters or instructions to  
9 staff, or (3) because they describe guidelines whose risk of circumvention is  
10 only apparent if it is presumed that one has obtained unauthorized access to  
11 the databases.

12 B. For all information withheld after segregating and releasing the nonexempt  
13 material described above, to provide such withheld information to the Court,  
14 along with detailed, nonconclusory, and specific justifications for why such  
15 information was withheld, for in camera review.

### 16 **III. ADEQUACY OF SEARCH**

17 The Court finally finds that CBP has not proved it conducted adequate searches for records  
18 responsive to Plaintiff's Privacy Act and FOIA requests. An agency must produce specific evidence  
19 that proves that it has conducted a search reasonably calculated to uncover all relevant documents  
20 requested. Zemansky v. EPA, 767 F.2d 569, 571 (9th Cir. 1985). The agency's burden of proof is  
21 the same under either FOIA or the Privacy Act. Lane v. Dep't of Interior, 523 F.3d 1128, 1139 & n.9  
22 (9th Cir. 2008).

23 The adequacy of an agency's search for documents is judged by a reasonableness standard,  
24 with the facts construed in the light most favorable to the requester. Zemansky, 767 F.2d at 571;  
25 Steinberg v. Dep't of Justice, 23 F.3d 548, 551 (D.C. Cir. 1994). A search will be considered  
26 adequate only if the agency has made a "good faith effort to conduct a search for the requested  
27 records, using methods which can be reasonably expected to produce the information requested."  
28 Oglesby v. Dep't of Army, 920 F.2d 57, 68 (D.C. Cir. 1990).



1           **A.     Hasbrouck’s 2007 Privacy Act request for his ATS records and 2009 request for**  
2           **his ATS, TECS, BCIS, and APIS records**

3           CBP’s FOIA Branch conducted two searches in response to Hasbrouck’s Privacy Act  
4 requests for his travel-related records. CBP does not explain how that search was conducted. A  
5 second search was conducted in December 2009. CBP has not carried its burden of proving that this  
6 search was adequate either. Instead CBP simply concludes (twice) that “all files likely to contain  
7 responsive material were searched.” [Suzuki Decl. ¶¶ 16, 18-20] CBP’s bare conclusion is not  
8 sufficient.

9           Nor did CBP use search parameters that were reasonably calculated to discover responsive  
10 records. CBP searched ATS and TECS using only the search terms “Hasbrouck,” “Edward,” and his  
11 date of birth. [Suzuki Decl. ¶ 16] CBP did not search using alternative spellings of his name, even  
12 though it does that in other situations [Suzuki Decl. ¶ 16], and even though CBP can employ a  
13 “LIKE” names search option in searching TECS and ATS. [Hasbrouck Decl. ¶ 57] Given that  
14 “Hasbrouck” is frequently misspelled [Hasbrouck Decl. ¶¶ 51, 53-54], is subject to numerous  
15 alternative spellings [Hasbrouck Decl. ¶ 52], and that PNR records are known to be so fraught with  
16 misspelled names that alternative spelling searches are the norm in the travel industry [Hasbrouck  
17 Decl. ¶ 56], CBP’s failure to do such a search was unreasonable. CBP also did not conduct a  
18 transposed name search, even though it does search for different name combinations in some  
19 circumstances. [Suzuki Decl. ¶ 16] Transposed names are one the most common reasons why PNR  
20 data is not located in the commercial context. [Hasbrouck Decl. ¶ 60] Finally, CBP failed to search  
21 by Hasbrouck’s passport number or telephone number, searches that are commonly understood in  
22 the travel industry as providing more complete results in finding PNR data than name searches.  
23 [Hasbrouck Decl. ¶ 59]

24           Similarly, CBP’s Privacy Branch did not perform an adequate search. Following CBP’s  
25 August 2007 release of 16 pages of records to Hasbrouck, Hasbrouck appealed by letter dated  
26 September 13, 2007, specifying that an adequate search would have included several specific  
27 categories of information. [Hasbrouck Decl. Exh. C] In response, the CBP Privacy Branch conducted  
28 what it called an “intensive and encompassing” search in February and March 2009. [Castelli Decl.

1 ¶ 13] As with the FOIA Branch, CBP has not carried its burden of proving that this search was in  
2 fact adequate.

3 For records pertaining to Hasbrouck as a traveler, 20 pages of records were identified as  
4 responsive and produced to Hasbrouck in March 2009. [Castelli Decl. ¶¶ 13-15] But CBP provides  
5 no information about how such records were searched for, identified or located.

6 Only scant more detail is provided for the records pertaining to Hasbrouck as a travel agent.  
7 Aside from indicating that it used some of the search terms suggested by Hasbrouck in his appeal  
8 letter, [Castelli Decl. ¶ 13] CBP tells the Court little about that search. CBP's explanation here is  
9 similarly deficient.

10 Finally, aside from employing some of the search terms suggested by Hasbrouck, there is no  
11 indication that any of the other points included in Hasbrouck's appeal letter were addressed.

12 **B. Hasbrouck's 2009 Privacy Act/FOIA request for records of the processing of his**  
13 **2007 Privacy Act request and appeal**

14 CBP has failed to establish that it conducted an adequate search for records in response to  
15 Hasbrouck's 2009 Privacy Act/FOIA request for records regarding the processing of his 2007 FOIA  
16 request and appeal thereof. CBP's contention that it found no responsive records is not believable.  
17 Its own evidence refers to numerous communications within CBP that were made regarding  
18 Hasbrouck's 2007 Privacy Act request. Moreover, there is evidence that other records of the  
19 processing of Hasbrouck's 2007 Privacy Act request and appeal must also exist.

20 **C. Hasbrouck's 2009 FOIA request for documents describing search systems and**  
21 **methods**

22 CBP has not carried its burden of proving that it adequately searched for records in response  
23 to Hasbrouck's 2009 FOIA request for records relating to the search and retrieval of records from  
24 ATS, APIS, BCIS and TECS. In response, CBP only located and produced wholly redacted versions  
25 of the TECS and ATS user guides. [Suzuki Decl. ¶ 22]

26 This search is inadequate because Hasbrouck sought more than just user guides. In addition  
27 to "user manuals, training manuals or materials, reference manuals, query format guides, search  
28 protocols or instructions, interpretation guides, standard operating procedures," Hasbrouck also

1 specified “contract specifications, software use cases or other functional or technical specifications,  
2 Application Programming Interface specifications and formats for any software or systems which  
3 contain, process, or interact with these records.” CBP has not explained how it searched for such  
4 software specifications, if it searched at all.

5 Accordingly, Defendant is hereby ORDERED:

6 A. With respect to Hasbrouck’s 2007 and 2009 Privacy Act requests for his  
7 ATS, TECS, BCIS, and APIS records:

8 1. To explain how its records are stored to enable the Court to assess  
9 whether all places reasonably likely to contain responsive records  
10 were searched and to explain whether any specific repositories were  
11 not searched and why;

12 2. To explain whether CBP uses a manual or computerized indexing  
13 system and how responsive records are otherwise identified, located,  
14 and searched;

15 3. To conduct searches in accordance with Hasbrouck’s June 27, 2007  
16 Privacy Act request letter, his August 13, 2007 appeal letter, and his  
17 October 15, 2009 request letter, by conducting searches in ATS and  
18 BCIS for records that include, but are not limited to:

19 a. all PNR data, including the “face” of each PNR, the  
20 “history” of each PNR, ticket records, and any other  
21 data retrievable from the PNR, whether or not that  
22 data is displayed on the “face” of the PNR;

23 b. information about Hasbrouck contained in PNRs for  
24 his own travel as well as any information about him in  
25 PNRs for other individuals’ travel, such as “split”  
26 PNRs cross-referenced with the record locators of  
27 PNRs for his travel, and any other PNRs that contain  
28 Hasbrouck’s identifying particulars as set forth in his

1 request letters;

2 using parameters that include, but are not limited to:

3 a. Hasbrouck’s name, address, date and place of birth,  
4 current and past passport numbers, and current and  
5 past telephone numbers;

6 b. identifying particulars of records pertaining to  
7 Hasbrouck in his capacity as a travel agent, including,  
8 but not limited to, all PNRs from the Sabre CRS/DHS  
9 showing PNR history entries from pseudo-city code  
10 A787 (including owner, creator, and history entries)  
11 and agent sines A24 or AEH, and all records from the  
12 Sabre, Galileo/Apollo, Amadeus, or Worldspan  
13 CRSs/GDSs identifiable with ARC/IATA travel  
14 agency number 05626515 or agency “Airtreks,”  
15 “Airtreks.com,” or “High Adventure Travel,” and  
16 agent or “received” or agent phone entries including  
17 “EH” or “Edward” in the PNR or any PNR history  
18 entries;

19 c. variations of Hasbrouck’s name, including but not  
20 limited to “HASBROUCK/EDWARD JOHN,”  
21 “HASBROUCK/EDWARD J,” “HASBROUCK  
22 /EDWARD,” “HASBROUCK/EDWARD JOHN  
23 MR,” “HASBROUCK/EDWARD J MR,” AND  
24 “HASBROUCK/EDWARD MR”;

25 d. transpositions for each of the variations indicated  
26 above, including but not limited to “LAST  
27 NAME/FIRST NAME” and “FIRST NAME/LAST  
28 NAME”;

1 e. searches taking in account misspellings and data entry  
2 errors using “similar” or “like” names and any  
3 available “fuzzy matching” capacity;

4 f. searches for PNRs and another records for  
5 Hasbrouck’s name and identifying particulars in any  
6 indexed fields or fields by which data may be  
7 retrieved, not just solely by name in the “name” field.

8 B. With respect to Hasbrouck’s 2009 Privacy Act/FOIA request for records of  
9 the processing of his 2007 Privacy Act request and appeal:

10 1. To produce records in which the case file number H051659 is  
11 assigned to Hasbrouck’s 2007 Privacy Act request when the request  
12 was referred from the FOIA Division to the Privacy Branch on  
13 February 2, 2009, and other records of the referral or the assignment  
14 of the case file number;

15 2. To produce records documenting the transfer of the appeal of the  
16 2007 Privacy Act request from the FOIA Branch to the Privacy  
17 Branch following a February 2009 telephone call with Hasbrouck;

18 3. To produce e-mail communications between the Privacy Branch and  
19 the Office of Intelligence and Operations Coordination (OIOC) on  
20 February 25, 2009, March 30, 2009, and April 2, 2009;

21 4. To search for and produce records of the Privacy Branch, whose  
22 records were not searched by the FOIA Branch because it simply told  
23 Hasbrouck to contact the Privacy Branch himself;

24 5. To search for and produce records found in audit logs generated  
25 during the processing of the 2007 Privacy Act request;

26 6. To search for and produce records of Hasbrouck’s e-mail exchange  
27 with Hugo Teufel, John Kropf, and Vania Lockett regarding  
28 Hasbrouck’s request, or any records of Teufel, Kropf, or Lockett

1 having investigated the status of Hasbrouck's request;

2 7. To search for and produce records of numerous telephone calls made  
3 from mid-2008 to early 2009 between Hasbrouck and CBP and DHS  
4 in Hasbrouck's attempt to learn the status of his 2007 request;

5 8. To search for and produce Hasbrouck's original signed 2007 request  
6 and appeal;

7 9. To search for and produce other records responsive to Hasbrouck's  
8 2009 Privacy Act/FOIA request for records of the processing of his  
9 2007 Privacy Act request and appeal, in accordance with his October  
10 15, 2009 request letter, by searching for these records in locations  
11 including, but not limited to: e-mail archives, memo files, FOIA logs,  
12 Privacy Act logs, appeal logs, electronic database audit or access logs,  
13 or the personal files of the DHS employees involved, either in the  
14 FOIA Division, the FOIA Branch, the Privacy Branch or the  
15 Passenger Branch's OIOC.

16 C. With respect to Hasbrouck's 2009 FOIA request for documents describing  
17 search systems and methods, to re-search for and produce documents in  
18 accordance with his October 15, 2009 request letter, by searching for  
19 documents that include, but are not limited to: user manuals, training manuals  
20 or materials, reference manuals, query format guides, search protocols or  
21 instructions, interpretation guides, standard operating procedures, contract  
22 specifications, software use cases or other functional or technical  
23 specifications, Application Programming Interface specifications and formats  
24 for any software or systems which contain, process, or interact with the ATS,  
25 TECS, APIS, BCIS systems of records, as well as the contents of any online  
26 or electronic help or reference system for any of these systems.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

IT IS SO ORDERED.

Dated:

\_\_\_\_\_  
Richard Seeborg  
United States District Judge