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

PLAINTIFF'S REPLY MEMORANDUM IN SUPPORT OF HIS CROSS-MOTION FOR SUMMARY JUDGMENT

Date: August 25, 2011
Time: 1:30 PM
Courtroom: 3

Judge: The Hon. Richard Seeborg

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

United States Code

FEDERAL REGISTER

LEGISLATIVE HISTORY

Senate Reports

House Reports

/ / /

/ / /

/ / /

INTERNATIONAL AUTHORITIES

OTHER AUTHORITIES

SUPPLEMENTAL STATEMENT OF FACTS

A passenger name record (PNR) in the database of a travel company may contain information about multiple travel services (flights, hotels, etc.) entered by multiple travel companies. Travelers rarely enter data directly in PNRs, and typically do not know and cannot control what data is included in PNRs. There are typically multiple intermediaries between the traveler and the Computerized Reservation System (CRS) in which the PNR is stored. Spelling and transcription errors can be introduced at each stage of transmission of PNR data, such as between a retail travel agency and an airline ticket wholesaler or "consolidator," who may be located overseas and have limited English-language skills. Staff of each of the companies participating in a PNR can enter data in the PNR, including unlimited free-text "remarks." Airlines are required to make available to CBP the entire PNRs of all passengers transported across U.S. borders. These PNRs then become part of CBP's ATS system of records. PNRs imported into ATS can include, for example, credit card numbers, names of traveling companions, and potentially derogatory personal comments and descriptions of interactions with customer service staff.[1]

Acknowledging the sensitivity of the data in PNRs, Canadian and European Union laws require that private entities that control or host PNRs allow individuals to inspect their own PNRs and obtain information about how they are used.[2] However, U.S. law contains no such requirement.

Given the way in which the PNRs that are obtained by CBP are created, it is incorrect to assert, as CBP has, that "the PNR records in ATS-P consist of information that is supplied either directly by the traveler or at his/her direction," or to conclude that misspellings are unlikely or limited to cases in which a traveler misspells his or her own name. [Castelli Supp. Decl. ¶ 10][3]

[1] See 2d Hasbrouck Decl. ¶¶ 12-15, 19-21, 24-27, 30. See also Edward Hasbrouck, "What's in a PNR?," http://hasbrouck.org/articles/PNR.html (last visited July 28, 2011).

[2] See Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5, § 5 (Can.); Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 12, 1995 O.J. (L 281) 31; Regulation No. 80/2009 of the European Parliament and of the Council on a Code of Conduct for Computerised Reservation Systems, art. 11, 2009 O.J. (L 35) 47 (EC).

[3] CBP takes issue with the extent of Hasbrouck's expertise regarding the ability to query the ATS. [Def's Opp. at 1-2] However, the CBP personnel, although having knowledge of how

ARGUMENT

I. CBP HAS NOT COMPLIED WITH THE PRIVACY ACT BECAUSE THE 2010 REGULATIONS EXEMPTING ATS, BCIS, AND FOIA AND PRIVACY ACT PROCESSING RECORDS FROM THE PRIVACY ACT DO NOT OPERATE RETROACTIVELY AND THUS DO NOT APPLY TO HASBROUCK'S 2007 AND 2009 PRIVACY ACT REQUESTS

A. CBP IS BARRED FROM ADOPTING RETROACTIVE PRIVACY ACT REGULATIONS BECAUSE CONGRESS HAS NOT GIVEN IT THE POWER TO DO SO

As set forth in Hasbrouck's opening memorandum, CBP has not complied with the Privacy Act because it has treated much of the ATS and the entire BCIS as exempt from the Privacy Act's disclosure and accounting requirements. CBP now additionally asserts that it did not produce certain emails regarding the processing of Hasbrouck's 2007 Privacy Act request and appeal because such records were exempted from the Privacy Act by another 2010 rulemaking.[4] CBP's contention must be rejected because the 2010 rulemakings that created such exemptions do not properly apply retroactively to Privacy Act requests made prior to the promulgation of those regulations.

An agency cannot promulgate retroactive regulations unless Congress has given the agency that power "in express terms." Bowen v. Georgetown Univ. Hosp., 488 U.S. 204, 208 (1988). See Newman v. Apfel, 223 F.3d 937, 942 (9th Cir. 2000) (describing Bowen as establishing "an absolute bar against an agency's retroactive rulemaking absent statutory authority"). This bar on agency action is a necessary result of the axiom that "an administrative agency's power to promulgate legislative regulations is limited to the authority delegated by Congress." Bowen, 408 U.S. at 208. And it is a necessary result of the definition of a "rule" contained in the Administrative Procedures Act as meaning "the whole or a part of an agency statement of general or particular applicability *and future effect* designed to implement, interpret, or prescribe law or policy or describing the organization,

information is stored in ATS, have provided no foundation for their numerous statements regarding the way the travel industry creates the records that are provided to CBP. [2d Hasbrouck Decl. ¶¶ 17, 18]

[4] CBP contends "that the email records system is exempt from the access provision of the Privacy Act." [Def's Opp. at 18:13-14; Castelli Supp. Decl. ¶ 13] CBP provides no authority for this exemption, but is apparently relying on 75 Fed. Reg. 50846, 50846-50847 (Aug. 18, 2010). That regulation exempted FOIA and Privacy Act processing records from the Privacy Act.

procedure, or practice requirements of an agency . . . ." 5 U.S.C. § 551(4) (emphasis added); Bowen, 488 U.S. at 216-18 (Scalia, J., concurring) ("In short, there is really no alternative except the obvious meaning, that a rule is a statement that has legal consequences only for the future.").

Thus, unlike an inquiry into the retroactivity of a *statute,* the "threshold question" in examining the purported retroactivity of an *administrative regulation* is whether the law from which the agency's lawmaking authority is derived "authorizes retroactive rulemaking." Bowen, 408 U.S. at 208. See also Cort v. Crabtree, 113 F.3d 1081, 1084 (9th Cir. 1997) (explaining, although not deciding, Bowen's requirement that "courts must determine as a threshold matter whether retroactive rulemaking exceeds the agency's statutory grant of rulemaking authority"). If the law contains no such express authorization, the agency's action is *ultra vires*.

The Privacy Act contains no such express authorization, neither at subsections (j)(2) or (k)(2) nor anywhere else. Indeed, to the contrary, the legislative history[5] indicates that Congress intended that exemptions to the Privacy Act be applied prospectively only: "We have made sure that systems may be exempted from certain requirements of the bill *only after* the head of an agency promulgates rules which are open to public comment *before they become effective*." S. Rep. No. 93-1416, at 18 (1974) (emphasis added).[6]

CBP thus lacks the authority to promulgate rules retroactively exempting a system of records from the provisions of the Privacy Act. The 2010 rules exempting ATS, BCIS and FOIA/Privacy Act processing records thus cannot be applied to Hasbrouck's 2007 and 2009 Privacy Act requests.

B. EVEN IF THE THRESHOLD ISSUE OF CONGRESSIONAL AUTHORITY COULD BE OVERCOME, THE REGULATIONS WOULD HAVE IMPROPER RETROACTIVE EFFECTS

Only if the threshold requirement of rulemaking authority is satisfied does the court move on to the question of whether the regulation can properly be given retroactive application, following the two-part test set forth in Landgraf v. USI Film Prods., 511 U.S. 244, 280 (1994).

[5] When the statute is silent as to retroactivity, the legislative intent may be discerned from the legislative history. Koch v. SEC, 177 F.3d 784, 786 n.3 (9th Cir. 1999).

[6] As CBP acknowledges, the only reference to temporality found in the Privacy Act indicates Congress's disinclination to allow for retroactive application of the law's provisions. See 5 U.S.C. § 552a(g)(5). [Def.'s Opp. at 13:9-12]

However, even if this Court were to conduct that analysis, the result would be the same: the exemptions do not apply to Hasbrouck's Privacy Act requests.

In Landgraf, the Supreme Court sought to reconcile the apparent tension between two canons of statutory construction: one from Bowen that "congressional enactments and administrative rules will not be construed to have retroactive effect unless *their language* requires this result"[7]; and one from Bradley v. School Bd. of Richmond, 416 U.S. 696, 711 (1974), that "a court is to apply the law in effect at the time it renders its decision." Landgraf, 511 U.S. at 264 (emphasis added). The Court concluded that non-retroactivity must be presumed and that Bradley merely described examples, to wit, "many situations," of when that presumption might be overcome. Id. at 277 ("[W]e now make it clear that Bradley did not alter the well-settled presumption against application of the class of new statutes that would have genuinely 'retroactive' effect."). See also id. at 278 ("[W]e did not intend [in Bradley] to displace the traditional presumption against applying statutes affecting substantive rights, liabilities, or duties to conduct arising before their enactment.").[8]

The Court thus set up a two-part analysis. First, a court will look to see whether the statute or regulation itself, by its express language or implied intent, mentions temporality. If it does, a court will defer to that statement. Landgraf, 511 U.S. at 280. If the statute or regulation itself is silent, the presumption against retroactivity applies and will be overcome only if the application of the new

[7] Neither Landgraf nor Bradley, both of which considered the retroactivity of statutes, addressed Bowen's threshold determination of whether an administrative agency had the Congressional authority to enact a retroactive regulation. See Landgraf, 511 U.S. at 265 (explaining that the *holding* of Bowen, that the agency lacked Congressional authority, was not in conflict with the holding of Bradley). Rather they looked at what happens if that precondition is met and a court must then examine the regulation, and *its* language, to determine if the regulation itself expressly requires a retroactive application.

[8] In contrast, judicial decisions are applied retroactively. Landgraf, 511 U.S. at 278 n.32 "'The principle that statutes operate only prospectively, while judicial decisions operate retrospectively, is familiar to every law student,' United States v. Security Industrial Bank, 459 U.S. 70, 79 (1982), . . . 'Judicial decisions have had retrospective operation for near a thousand years.' [Kuhn v. Fairmont Coal Co., 215 U.S. 349, 372 (1910) (Holmes, J., dissenting)]." Rivers v. Roadway Express, Inc., 511 U.S. 298, 311 (1994). CBP's suggestion that its regulatory exemptions be applied retroactively because the Supreme Court's decision barring it from asserting the "high 2" FOIA exemption is applied retroactively must thus be rejected. See Milner v. Dep't of Navy, 131 S. Ct. 1259, 1271 (Mar. 7, 2011).

regulation would not "impair rights a party possessed when he acted, increase a party's liability for past conduct, or impose new duties with respect to transactions already completed." Id. at 280. See Koch, 177 F.3d at 785-86 & n.3. And indeed, even enactments that do not have one of these specific, impermissible effects may be found to operate prospectively only. Hughes Aircraft Co. v. United States, 520 U.S. 939, 947 (1997) (holding that the Landgraf factors were not intended to be the "exclusive definition of presumptively impermissible retroactive legislation"). "The conclusion that a particular rule operates 'retroactively' comes at the end of a process of judgment concerning the nature and extent of the change in the law and the degree of connection between the operation of the new rule and a relevant past event." Landgraf, 511 U.S. at 270.

Although there are no brightline rules for which types of statutes or regulations overcome or fail to overcome the presumption against retroactivity, the Court in Landgraf did set forth some general categories which are of use to this Court considering the purported retroactivity of the CBP Privacy Act exemptions.

As a general matter, the following types of laws may be given retroactive effect: (1) laws that remove a burden on private rights, id. at 270-71, 276 n.30; (2) laws that affect the propriety of prospective relief, id. at 273; (3) laws conferring or ousting jurisdiction, id. at 274; (4) laws changing procedural rules, id. at 275; and, (5) laws pertaining to issues that are collateral to and uniquely separable from the main cause of action, id. at 277.

As a general matter, the following types of laws will *not* be given retroactive effect absent clear language to the contrary: (1) laws burdening private rights, as opposed to laws that give a benefit to the public as a whole; (2) laws that impose new burdens on persons after the fact; and, (3) laws affecting contractual or property rights. Id. at 270-71. But even beyond these general categories, "prospectivity remains the appropriate default rule." Id. at 272-73.

In this case, this default rule should prevail and CBP's Privacy Act regulations divesting citizens of their personal rights with respect to ATS, BCIS and FOIA/Privacy Act processing records must not be applied retroactively to requests pending before the promulgation of the 2010 rules.

In drafting the Privacy Act, Congress intended to "promote accountability, responsibility, legislative oversight, and open government" with respect to personal information. S. Rep. No.

93-1183, at 1 (1974). The Privacy Act is "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies." Id.

The ability of individuals to access records kept on them by the government is the Privacy Act's primary mechanism of enforcement of these aims. See id. at 3 (noting that Privacy Act gives individuals the right to access government records on them "to aid in the enforcement of these legislative restraints"). See also Henke v. Dep't of Commerce, 83 F.3d 1453, 1456 (D.C. Cir. 1996) (noting that the "main purpose" of the Privacy Act access provision is to afford individuals an opportunity to review and correct personal information). As a result, "[e]xemption from the Privacy Act's fundamental requirement that an individual have access to an individual's 'record or to any information pertaining to him' collected by the government is a serious matter." Louis v. Dep't of Labor, 419 F.3d 970, 977 (9th Cir. 2005).

That these formerly vested private rights secured by the Privacy Act would be improperly defeated by the retroactive application of CBP's exemptions is evident when the Privacy Act is compared with FOIA. The two statutes were designed to serve different goals: "[T]he FOIA was enacted to provide citizens with better access to government records, while the Privacy Act was adopted to safeguard individuals against invasions of their privacy." Flowers v. Exec. Office of the President, 142 F. Supp. 2d 38, 42 (D.D.C. 2001). Additionally, "[t]he Privacy Act—unlike the Freedom of Information Act—does not have disclosure as its primary goal." Henke, 83 F.3d at 1456. "Rather, the main purpose of the Privacy Act's disclosure requirement is to allow individuals on whom information is being compiled and retrieved the opportunity to review the information and request that the agency correct any inaccuracies." Id. at 1457 (citing 5 U.S.C. § 552a(d)(2)). These differences mirror the private rights–public rights dichotomy often seen in the retroactivity cases.[9]

[9] Thus, although the adequacy of search standards under the laws have been found to be similar, Lane v. Dep't of Interior, 523 F.3d 1128, 1139 n.9 (9th Cir. 2008), "there is nothing in either statute or in the relevant legislative history that requires courts to resolve claims arising under the Privacy Act pursuant to standards developed to assess claims arising under FOIA." Blazy v. Tenet, 194 F.3d 90, 92 (D.C. Cir. 1999).

CBP's reliance on Southwest Ctr. for Biological Diversity v. Dep't of Agriculture, 314 F.3d 1060, 1061 (9th Cir. 2002), in which the court gave a highly specific FOIA exemption retroactive effect, is thus misplaced. A retroactive FOIA exemption burdens only an individual's ability to "request or sue for information." Id. at 1062. In contrast, a retroactive Privacy Act exemption eliminates an individual's ability to review and correct inaccuracies in records kept about him or her by the government and to know how the government distributed any information collected.

Perhaps most importantly, unlike a FOIA exemption, a retroactive Privacy Act exemption will defeat an individual's expectations that existed when he or she submitted the information that was to ultimately end up in the hands of the government. Those making international travel arrangements might have chosen to use a foreign travel agent who would be required by foreign law to disclose what information they had entered in the PNRs, or avoid making flight and hotel or other arrangements in the same PNR, or take any number of other steps to limit, control, or retain the ability to know what information was included in PNRs that would be imported into their ATS records. Hasbrouck himself would have taken such steps had he known that he could not use the Privacy Act to safeguard his privacy rights.[10] [2d Hasbrouck Decl. ¶¶ 5-9]

Thus, even if this Court were to look beyond the absence of Congressional authorization to enact retroactive Privacy Act regulations, the presumption that the regulations not be applied retroactively must prevail.

///

///

[10] CBP's claim that retroactivity would not be unfair because its intent to exempt was published in a Notice of Proposed Rule Making [Def.'s Opp. at 14:22-23] must also be rejected. Hasbrouck's 2007 Privacy Act request was submitted on June 27, 2007, before the NPRM was published on August 6, 2007. Moreover, there were many public comments objecting to the proposed objection, including one submitted by Hasbrouck. An agency has a statutory duty to consider those comments. An individual may thus rightfully assume that the agency might adjust its proposed rule in light of them. [2d Hasbrouck Decl. ¶¶ 1-4]

The retroactive application of the ATS and BCIS exemptions is especially egregious in this case where the processing of Hasbrouck's Privacy Act requests was completed by CBP's Office of Intelligence and Operation Coordination on April 2, 2009, but was then sat on for 17 months until after the exemption rules were finalized. [Castelli Decl. ¶¶ 14-15]

II. CBP DID NOT COMPLY WITH FOIA BECAUSE IT IMPROPERLY WITHHELD NONEXEMPT MATERIAL FROM DISCLOSURE

A. HASBROUCK REQUESTS ONLY THAT VERY LIMITED INFORMATION BE SEGREGATED FROM THE USER GUIDES

The Privacy Act requires that all agency records retrievable by an individual's name or *personal identifier*[11] be maintained in a "Privacy Act System of Records." Nation Magazine v. Customs & Border Protection, 71 F.3d 885, 890 n.4 (D.C. Cir. 1995). In its SORN for ATS, CBP states, "The data is retrievable by name or *personal identifier* from an electronic database." 72 Fed. Reg. 43650, 43654 (Aug. 6, 2007) (emphasis added). In its SORN for TECS, CBP states, "The data is retrievable by name, address, *unique identifiers* or in association with an enforcement report or other system document." 73 Fed. Reg. 77778, 77782 (Dec. 19, 2008) (emphasis added).

Through this motion, Hasbrouck seeks very limited information: a list of these "personal" and "unique" identifiers by which data can be retrieved from an individual's ATS, APIS, BCIS, ADIS, and TECS records. This list might include, for example, family names, first names, addresses, dates of birth, passport numbers, credit card numbers, telephone numbers, etc.

It must be possible to segregate such a list from the user guides that have been identified as responsive to his FOIA request. This list of "personal" and "unique" identifiers may well be the only words left un-redacted on the page, if such redactions are truly necessary to maintain the security of the systems. The resulting document may seem like "unintelligible gibberish" to CBP [Suzuki Supp. Decl. ¶ 18] but it will be meaningful to Hasbrouck, and to the public in general.

Hasbrouck does not seek instructions, "step-by-step," or otherwise, on how to navigate or retrieve data from the records systems.[12] He does not seek the entire user guides or suggest that entire user guides be published in the Federal Register.

[11] The specific language in the Privacy Act is "name, or the identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(4) (defining "record"), § 552a(a)(5) (defining "systems of records"). Hasbrouck used this exact language in his 2009 FOIA request for information regarding retrievability. [Suzuki Decl. Exh. F] The term "personal identifier" is used to refer back to these definitions in section 552a(a)(8)(B)(1).

[12] CBP's statements that Hasbrouck was seeking only records that would "explain how to retrieve information from the system" is thus incorrect. [Suzuki Supp. Decl. ¶¶ 14, 20]

B. THE PRIVACY ACT REQUIRES THAT "POLICIES AND PRACTICES" REGARDING "RETRIEVABILITY" BE MADE PUBLIC

As set forth in Hasbrouck's opening memorandum, the Privacy Act requires that agencies publish in the Federal Register "the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records" in a system of records. 5 U.S.C. § 552a(e)(4)(E).

No court has yet interpreted the meaning of "policies and practices" in this provision of the Privacy Act. But the legislative history indicates that Congress intended to require that agencies "adequately" inform the public as to the policies "governing the physical custody and protection of the record systems." H.R. Rep. No. 93-1416, at 16 (1974) (discussing former subsection (e)(2), renumbered in the final statute as subsection (e)(4)). "Policies and practices" must include more than the highly generalized statements CBP published in its SORNs. The Privacy Act must require that CBP specify what these "personal" and "unique" identifiers are; the SORN, as written, provides almost no useful information to the public.

Thus, to the extent that the user guides contain "policies and practices regarding . . . retrievability," such information must be segregated and released. This should include the list of "personal" and "unique" identifiers by which data can be retrieved from the records systems sought here by Hasbrouck. This Court should order CBP to produce a list of the "personal" and "unique' identifiers referred to in the SORNs from the user guides.

C. THIS COURT SHOULD REVIEW THE USER GUIDES IN CAMERA TO DETERMINE WHETHER THERE IS ANY SEGREGABLE RESPONSIVE INFORMATION THAT CAN BE PRODUCED

Alternatively, this Court may review the user guides *in camera* to determine whether the "personal" and "unique" identifiers can be segregated from the exempt information. In so doing, this Court may employ the standards set forth in Hasbrouck's opening memorandum by which nonexempt information is distinguished from exempt information for the purposes of exemption (7)(E). *In camera* review is common in FOIA cases because the party seeking disclosure cannot know the precise contents of the records, and the court is thus deprived of fully informed advocacy. See Vaughn v. Rosen, 484 F.2d 820, 823 (D.C. Cir. 1973) ("Obviously the party seeking disclosure cannot know the precise contents of the documents sought; secret information is, by definition, unknown to the party seeking disclosure."); Weiner v. FBI, 943 F.2d 972, 977 (9th Cir. 1991) ("The party requesting disclosure must rely upon his adversary's representations as to the material withheld, and the court is deprived of the benefit of informed advocacy to draw its attention to the weaknesses in the withholding agency's arguments.").

III. CBP FAILED TO SEARCH ADEQUATELY FOR RECORDS RESPONSIVE TO HASBROUCK'S REQUESTS

A. CBP ADMITS THAT NUMEROUS REQUESTED RECORDS EXIST BUT WERE NOT SEARCHED FOR

CBP admits that there are numerous responsive records for which it did not search.

1. SOFTWARE SPECIFICATIONS

In his 2009 FOIA request, Hasbrouck specifically requested "contract specifications, software use cases or other functional or technical specifications, Application Programming Interface (API) specifications and formats for any software or systems which contain, process, or interact with these records" that contain the "identifying particulars by which Passenger Name Record (PNR) or other data can be retrieved from ATS, APIS, BCIS, ADIS, and TECS." [Suzuki Decl. Exh. F] Nevertheless, CBP refused to even search for responsive information in the software specifications because "they would not explain how to retrieve information from the databases." [Suzuki Supp. Decl. ¶ 14] However, as explained above, Hasbrouck is not seeking records of "how to retrieve information from the databases," but rather the personal identifiers by which information may be retrieved from the databases. Hasbrouck specifically asked for software specifications in his FOIA request because one would expect that the person designing the software would be told what the desired unique identifiers are. It is unreasonable for CBP to refuse to even search for them.

2. RECORDS RESPONSIVE TO HASBROUCK'S 2009 FOIA/PRIVACY ACT REQUEST FOR RECORDS PERTAINING TO THE PROCESSING OF HIS 2007 PRIVACY ACT REQUEST

a. SEARCH LOGS

CBP admits that search logs, that is, records of the searches performed for any reason on ATS and TECS, "are internally generated and used to 'police' the use of" those systems of records. [Suzuki Supp. Decl. ¶ 11] But CBP did not search for these clearly responsive records because these system access logs were not "intended nor designed to be used to" respond to FOIA and Privacy Act requests.[13] [Suzuki Supp. Decl. ¶ 11]

The intent or design of a record is not relevant to whether the records are responsive to a FOIA request. Indeed, one would imagine that most records systems are not "designed" for such purposes. But neither FOIA nor the Privacy Act limits its reach in the way CBP suggests.

b. SIGNIFICANT ACTIVITY REPORTS

CBP admits that it did not search for any "significant activity reports" pertaining to Hasbrouck's 2007 request and appeal therefrom. However, its reasons for failing to even look for these reports is inadequate. Suzuki states without any foundation, elaboration or explanation that, with respect to Hasbrouck's 2007 Privacy Act request, it is "unlikely it would have been reported as significant." [Suzuki Supp. Decl. ¶ 10] This cursory and unfounded explanation is not sufficient to justify the failure to even search for such records.[14]

c. CORRESPONDENCE BETWEEN CBP AND DHS

Hasbrouck reasonably expects that there should be records of correspondence between certain officials at DHS and the units of CBP charged with processing his 2007 Privacy Act request and the appeals therefrom because he was assured by the DHS officials that they would investigate the status

[13] See also 72 Fed. Reg. 43650, 43654 (Aug. 6, 2007) (stating in ATS SORN that ATS uses "auditing software" and "monitors source systems for changes to the source data"); Privacy Impact Assessment for the Automated Targeting System (2007), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats_updated_fr.pdf, at 16 (stating that "ATS retains audit logs for all user access"); Privacy Impact Assessment for the TECS System (2010), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_tecs.pdf, at 16 ("Extensive audit logs are maintained showing who has accessed records and what changes, if any, were made to the records."), and at 22 (stating that "TECS maintains audit trails or logs for the purpose of reviewing user activity").

[14] Based on the stated criteria, one would actually expect Hasbrouck's request to be deemed significant. As set forth in Hasbrouck's opening memorandum, "significant" FOIA requests were defined to include all requests for which: "The FOIA request or requested documents will garner media attention or is receiving media attention; . . . The FOIA request is from a member of the media; . . . FOIA request is from a member of an activist group, watchdog organization, special interest group, etc.;" or "The FOIA request is for documents associated with a controversial or sensitive subject." [Hasbrouck Opening Memo. at 23 n.20]

Hasbrouck's 2007 Privacy Act request, which CBP treated as a FOIA request, [Suzuki Decl. ¶ 8 & Exh. C] meets these criteria. The request was for documents associated with a controversial or sensitive subject. [Suzuki Decl. Exh. B] Moreover, Hasbrouck was and is known to CBP as a member of an activist/watchdog organization. [Hasbrouck Decl. Exh. W] of the request. [Hasbrouck Decl. ¶ 15] CBP has responded only that it has no access to DHS emails. [Suzuki Supp. Decl. ¶ 12] However, Hasbrouck is seeking emails between the DHS officials and CBP personnel. CBP cannot deny that is has access to such records. But CBP has not made any effort to search for them.

In other litigation, CBP has described "reading files," which hold copies of letters, memoranda, and correspondence, filed chronologically. See Nation Magazine v. Customs & Border Protection, 71 F.3d 885, 891 (D.C. Cir. 1995). CBP has not indicated whether it made any effort to search its "reading files" in response to Hasbrouck's request.

d. CORRESPONDENCE BETWEEN CASTELLI AND OIOC AND OTHER RECORDS OF THE PRIVACY BRANCH

CBP acknowledges the existence of email correspondence between its OIOC unit and Laurence Castelli regarding the processing of Hasbrouck's Privacy Act request. [Castelli Decl. ¶¶ 10, 11, 12, 13] However, these records were not produced, even though these records are indisputably responsive to both the Privacy Act and FOIA component of Hasbrouck's 2009 request.

With respect to the processing of the request under the Privacy Act, both excuses given by CBP for failing to produce the emails must be rejected. First, CBP claims that the correspondence was neither searched for nor produced because the correspondence was not responsive to Hasbrouck's 2007 Privacy Act request. However, Hasbrouck sought these records not in his 2007 Privacy Act request but in his 2009 FOIA/Privacy Act request for records pertaining to the processing of his 2007 request; the records are indisputably responsive to that request. Second, CBP did not search for these records, or in any way process the 2009 request under the Privacy Act, because the system of records "in which such correspondence resides is exempt from the Privacy Act." [Castelli Supp. Decl. ¶ 13] However, as explained above, the rule exempting FOIA and Privacy Act processing records from the Privacy Act cannot be applied retroactively to Hasbrouck's pre-existing request. CBP should be ordered to process the 2009 request under the Privacy Act.

With respect to the processing of the records under FOIA, CBP admits that it determined that responsive records were determined to be at the Privacy Branch. However, it stopped at that determination and did not actually produce any records to Hasbrouck.[Suzuki Decl. ¶ 25] An agency improperly limits its search where one component of the agency knows that the record exists in another component and fails to refer the request. Natural Res. Def. Council v. Dep't of Def., 388 F. Supp. 2d 1086, 1101-02 (C.D. Cal. 2005).[15]

B. CBP'S SEARCH METHODOLOGY WAS NOT REASONABLY CALCULATED TO UNCOVER ALL RELEVANT RECORDS

With respect to Hasbrouck's 2007 and 2009 Privacy Act requests for his travel records, CBP has failed to demonstrate that its searches were reasonably calculated to discover all responsive records. Suzuki admits that CBP did not conduct searches using the terms and parameters provided by Hasbrouck in his request. [Suzuki Supp. Decl. ¶ 8] She explains that CBP ran searches using only Hasbrouck's first name, last name, and date of birth, claiming that such searches are most likely to retrieve all responsive records about an individual.[16] [Id.]

Such searches are insufficient in light of the nature of the systems being searched. Suzuki states that misspellings, similar pronunciations, and transpositions are used when there is a likelihood for misspelling, transposition, or when the request or record suggest that other records should exist. [Id.] Castelli similarly states that it is "unlikely that the Plaintiff would misspell his own name." [Castelli Supp. Decl. ¶ 10]

However, as explained above, there are numerous opportunities for misspellings during the creation of the PNRs that are ultimately forwarded to CBP. [2d Hasbrouck Decl. ¶¶ 20-21, 24-27] CBP has admitted that it searches for spelling variations for some individuals. [Suzuki Supp. Decl. ¶ 8] Its refusal to do so for Hasbrouck is unreasonable.[17]

[15] CBP claims that even if it had processed the Privacy Branch's records under FOIA it would have claimed either the deliberative process exemption, [Castelli Supp. Decl. ¶ 13] or exemption 2 [Def's Opp. at 18:13] and not produced them anyway. However, even if that were the case, CBP still had a duty to segregate and produce nonexempt material and list the exempt portions in its Vaughn index. It failed to do either.

[16] CBP has also given no indication that it has searched for split PNR data, even though such data was specifically listed in Hasbrouck's 2007 Privacy Act appeal and 2009 Privacy Act request. [Suzuki Decl. Exhs. D, E] Split PNRs 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. [2d Hasbrouck Decl. ¶ 30]

[17] Although CBP refused to search for Hasbrouck's records using its misspelling protocol, it devoted substantial resources to searching for all records containing the name "Edward." [Castelli Supp. Decl. ¶¶ 6-11] However, given that the standard practice in many countries is that PNRs include only first initials, not full first names, a first-name search is not reasonably calculated to

CBP's restrictive search method is also insufficient in light of the purpose for which the systems are kept. ATS, BCIS, APIS, and TECS are systems of records in which personal information relating to individuals are collected in order to further CBP's law enforcement and antiterrorism purposes. See 73 Fed. Reg. 77778, 77778-79 (Dec. 19, 2008) (TECS); 73 Fed. Reg. 68435, (Nov. 18, 2008) (APIS); 73 Fed. Reg. 43457, 43457 (July 25, 2008) (BCIS); 72 Fed. Reg. 43650, 43650-51 (Aug. 6, 2007) (ATS). Surely, if CBP were conducting searches into these systems as part of a law enforcement investigation, CBP would not restrict searches of the databases using only first name, last name, and date of birth. Nor would the investigator confine searches to just one spelling of a suspected terrorist's name. Given the capabilities of the system, there would be no additional burden imposed by running searches using the parameters Hasbrouck requested. If a requester is to have any meaningful access to records under the Privacy Act, an agency retrieving records in response to a request for these records should not be held to a lesser standard than what the agency itself would consider a diligent search when using the system of records for its intended purpose.

C. OTHER RECORDS LIKELY EXIST THAT WERE NOT PRODUCED

Suzuki states that "Plaintiff has not articulated which specific records he believes exists that CBP has not provided to him." [Suzuki Supp. Decl. ¶ 6] Hasbrouck has in fact set forth these specific records in both his initial requests and the subsequent appeals. They include (but are not limited to) the following:

a. FOIA request and appeal docket or log entries;

b. Privacy Act request and appeal docket or log entries;

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

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

e. 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;

f. Records of the CBP OIOC including e-mail messages;

retrieve all of Hasbrouck's records. [2d Hasbrouck Decl. ¶¶ 28, 29]

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

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

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

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

k. Risk assessments;

l. Rules used in determining risk assessments;

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

n. Information required to be included in SORNs, including information contained in software specifications, procurement contracts, and documentation, and in records of offices developing or supervising software development or contractors;

o. Records of Hasbrouck's original, signed and dated 2007 requests and appeals and records of the office(s) or individual(s) to which they were assigned; and

p. Some record of who Stephen Christensen, the person who signed for Hasbrouck's appeal letter, is and in what capacity he worked for CBP.

[2d Hasbrouck Decl. ¶ 36]

CONCLUSION

For the above-stated reasons, Hasbrouck's motion for summary judgment should be granted and CBP's motion for summary judgment should be denied.

Dated: July 29, 2011

FIRST AMENDMENT PROJECT

by: /s/

David Greene

Attorneys for Plaintiff Edward Hasbrouck