MELINDA HAAG (CSBN 132612)
United States Attorney
JOANN M. SWANSON (CSBN 88143)
Chief, Civil Division
NEILL T. TSENG (CSBN 220348)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102
Telephone: (415) 436-7155
FAX: (415) 436-6927
neill.tseng@usdoj.gov

Attorneys for Defendant
U.S. CUSTOMS AND BORDER PROTECTION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

EDWARD HASBROUCK, Plaintiffs, v. U.S. CUSTOMS AND BORDER PROTECTION, Defendant.	No. C 10-03793 RS **DEFENDANT'S OPPOSITION TO PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT AND REPLY IN SUPPORT OF DEFENDANT'S MOTION FOR SUMMARY JUDGMENT** Date: August 18, 2011 Time: 1:30 p.m. Place: Courtroom 3, 17th Floor, 450 Golden Gate Ave, San Francisco, California Honorable Richard Seeborg

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

FEDERAL STATUTES

I. INTRODUCTION.

CBP conducted numerous detailed searches for information based on plaintiff's various FOIA and Privacy Act requests. It properly withheld under FOIA Exemption 7(E) information which would disclose law enforcement techniques and procedures that could reasonably be expected to risk circumvention of the law. In doing so, it met the requirements for segregability. CBP also properly withheld information under Privacy Act Exemptions (j)(2) and (k)(2). Finally, the original and supplemental declarations of Shari Suzuki and Laurence Castelli show that CBP conducted adequate searches. Therefore, the court should grant defendant's motion for summary judgment (Doc. #31) and deny plaintiff's cross-motion for summary judgment (Doc. #37).

II. STATEMENT OF FACTS.

CBP believes the material facts have already been set forth in Def.'s MSJ (Doc. #31). CBP simply takes this opportunity to address certain facts submitted by plaintiff in Pl.'s MSJ (Doc. #37).

First, plaintiff holds himself out to be an "an expert on numerous travel-related issues." Pl.'s MSJ at 2:6 (citing Hasbrouck Decl. (Doc. #40) ¶¶ 1, 41). However, at least one court has found his information to be faulty. Plaintiff submitted an affidavit in In 't Veld v. Dep't of Homeland Sec., 589 F. Supp. 2d 16 (D.D.C. 2008), as "a 'travel expert' familiar with Passenger Name Records and Computerized Reservation Systems used in the travel industry." Id. at 20. The plaintiff in that case had requested, in pertinent part, all records concerning herself maintained in ATS-P and APIS. See id. at 18. In granting summary judgment for the defendant, the court found fault with Hasbrouck's affidavit:

> Mr. Dodson points out that Computerized Reservations Systems used in the travel industry are not same as the Passenger module of the Automated Targeting System used by Customs and Border Protection, and the systems are not queried in the same way. Most critically, the Automated Targeting System does not maintain complete replicas of Passenger Name Record data as it is stored in Computerized Reservations Systems. Mr. Hasbrouck's affidavit is based on the faulty assumption that these systems are the same.

Id. at 21 (internal citation and footnote omitted). The court further noted, "While Mr. Hasbrouck maybe an expert in Passenger Name Record data and Computerized Reservations Systems, he does not purport to be an expert in the Automated Targeting System or any of the other data systems

searched pursuant to the FOIA request in this case." Id. at 21 n.3.

Second, to the extent plaintiff suggests he should have received an "immediate response" to any of his requests, e.g., Pl.'s Mot. at 6:16, the fact is that plaintiff is far from the only FOIA or Privacy Act requester in CBP's queue. In fiscal year 2010, for instance, the FOIA Appeals, Policy and Litigation ("FAPL") Branch considered more than 800 cases and the FOIA Division answered more than 18,000 requests. Supp. Decl. of Shari Suzuki ("Supp. Suzuki Decl."), filed concurrently herewith, ¶ 3. Moreover, the Privacy Act contains no provisions addressing processing procedures or deadlines, nor requires a letter of acknowledgment with a corresponding case file number to be sent to plaintiff. Supp. Decl. of Laurence Castelli ("Supp. Castelli Decl."), filed concurrently herewith, ¶ 4.

III. ARGUMENT.

A. CBP Properly Withheld Pages From the TECS and ATS User Guides Under FOIA Exemption 7(E).

1. The Public Does Not Generally Know How to Navigate and Use the TECS and ATS Databases at Issue.

Plaintiff concedes that he is not challenging the redaction of information on pages 000001-16 described in the Vaughn Index. Pl.'s MSJ (Doc. #37) at 1 n.1. Thus, the only withheld information on the Vaughn Index he is challenging are those pages numbered 000017-187, which are certain pages from the TECS and ATS user guides. Those pages were properly withheld under FOIA Exemption 7(E).

Plaintiff "does not contest that the records at issue have a rational nexus with CBP's law enforcement purpose." Pl.'s MSJ at 10 n.14. Therefore, the only question with respect to Exemption 7(E) is whether the production of the TECS and ATS user guides "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). It is undisputed that the user guides would reveal techniques and procedures for law enforcement investigations or prosecutions, to wit, "a road map of how to use the law enforcement databases." Def.'s MSJ at 15:26-27 (citing Suzuki Decl. ¶ 40).

Plaintiff asserts that "at least some of the techniques or procedures are actually routine and well known to the public." Pl.'s MSJ at 14:2-3. But plaintiff does not cite any evidence showing that any techniques or procedures are routine or well known. In fact, they are not. It defies logic to suggest that "step-by-step instructions on how to navigate a law enforcement database, step-by-step instructions on how to retrieve records from a law enforcement database," and the other techniques and procedures described in Suzuki Decl. ¶ 40 are routine or well known. It is also misleading and wrong to characterize these techniques and procedures as nothing more than "how to use drop-down menus, perform searches and read search results." Pl.'s MSJ at 14:15. "These are not generic or basic drop-down menus but rather menus that show specific law enforcement queries." Supp. Suzuki Decl. ¶ 19. This is not Windows for Dummies being withheld; it is the user guides for sensitive law-enforcement databases.

The techniques and procedures at issue are not the kind that "would leap to the mind of the most simpleminded investigator." Rosenfeld v. Dep't of Justice, 57 F.3d 803, 815 (9th Cir. 1995) (citation omitted). In Rosenfeld, the court held that Exemption 7(E) did not apply to a pretext phone call because that investigative technique was "generally known to the public." Id. This case, by contrast, involves techniques and procedures much more obscure than a pretext phone call: detailed instructions on how to navigate and use sensitive law enforcement databases. Those detailed instructions are not generally known to the public, even if the public generally knows how to use computers. Thus, Exemption 7(E) applies. Cf. Asian Law Caucus v. U.S. Dep't of Homeland Sec., No. C 08-00842 CW, 2008 WL 5047839, at *4 (N.D. Cal. Nov. 24, 2008). (applying exemption 7(E) regarding investigative techniques relating to watchlists because "knowing about the general existence of government watchlists does not make further detailed information about the watchlists routine and generally known"); Unidad Latina en Accion v. U.S. Dep't of Homeland Sec., 253 F.R.D. 44, 52 (D. Conn. 2008) (applying Exemption 7(E) to internal planning documents and reasoning that, "while the public generally knows" of the use of surveillance techniques, "the details, scope, and timing of those techniques are not necessarily well-known to the public").

Finally, although Exemption 7(E) is "generally limited to techniques or procedures that are

not well-known to the public, even commonly known procedures may be protected from disclosure if the disclosure could reduce or nullify their effectiveness." Judicial Watch, Inc. v. U.S. Dep't of Commerce, 337 F. Supp.2d 146, 181 (D.D.C. 2004). Thus, even if the public generally knows how to navigate or use databases, the TECS and ATS user manuals would still be exempt from disclosure because they give specific instructions regarding those databases which could be used to reduce or nullify those databases' effectiveness. Cf. Asian Law Caucus, 2008 WL at *4 (exempting documents from disclosure because "the names of the databases, reports, modules and information about the operation of watchlists... could lead to circumvention of CBP law enforcement efforts or facilitate improper access to the database for the purpose of frustrating law enforcement functions"); Cozen O'Connor v. U.S. Dep't of Treasury, 570 F. Supp.2d 749, 785-86 (E.D. Pa. 2008) (applying 7(E) because subjects of investigation "could avoid or misdirect . . . investigations and implementation if they knew what databases and what government sources were being used to gather information about them").

2. FOIA Exemption 7(E) Does Not Require CBP to Show That Releasing the User Guides Would Risk Circumvention of the Law, But Even if It Did, CBP Has Made That Showing.

Exemption 7(E) applies to "records or information compiled for law enforcement purposes" if the production of such information "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7). The Ninth Circuit has not decided whether the phrase "could reasonably be expected to risk circumvention of the law" applies only to guidelines or also to techniques and procedures. Asian Law Caucus, 2008 WL 5047839, at *3. Courts have come out on both sides. See id. (collecting cases on both sides but ultimately not reaching the issue).

In Def.'s MSJ at 15, defendant discussed Allard K. Lowenstein Int'l Human Rights Project v. Dep't of Homeland Sec., 626 F.3d 678, 681 (2d Cir. 2010), in which the Second Circuit explained in detail why the risk-of-circumvention requirement does not apply to techniques and procedures. The Second Circuit, citing a Supreme Court case, reasoned that "basic rules of

grammar and punctuation dictate that the qualifying phrase modifies only the immediately antecedent 'guidelines' clause and not the more remote 'techniques and procedures' clause." Id. (citing Barnhart v. Thomas, 540 U.S. 20, 26 (2003)). The Second Circuit further elaborated that this interpretation was supported by the legislative history of the statute's amendments:

> The fact that the two clauses of the statute were introduced at different times (the first clause in 1974 and the second clause in 1986) and that the modifying language (requiring disclosure unless "such disclosure could reasonably be expected to risk circumvention of the law") was not part of the first clause as it was originally enacted reinforces the conclusion that the modifying language should be read as attaching only to the new basis for exemption that was created along with it.

Id. at 681-82. Plaintiff did not address Lowenstein Int'l Human Rights Project, or its detailed reasoning, at all in Pl.'s MSJ.

The cases plaintiff cites are not as persuasive as Lowenstein Int'l Human Rights Project. Neither of the two circuit court decisions (one unpublished) plaintiff cites in Pl.'s MSJ at 15 & 15 n.18 examined the language at issue, much less the underlying grammar, punctuation and legislative history, in any detail. See Davin v. U.S. Dep't of Justice, 60 F.3d 1043, 1064 (3d Cir. 1995); Catledge v. Mueller, 323 Fed.App'x 464, 466 (7th Cir. 2009). Thus, the better view is to adopt the thorough reasoning of the Second Circuit in Lowenstein Int'l Human Rights Project.

Ultimately, the court can avoid deciding this question because CBP has met the requirements of Exemption 7(E) under either interpretation. Even if CBP is required to show that disclosure of techniques and procedures could reasonably be expected to risk circumvention of the law, it has done so. Suzuki delineated the different kinds of information contained in the user manuals and explained at length how the user manuals "provide a road map of how to use the law enforcement databases." Suzuki Decl. ¶ 40. Unlike the database documents at issue in ACLU of Wash. v. U.S. Dep't of Justice, the user manuals here do not simply "reveal the location of information within [the agency's] databases and systems" without identifying "the data structures nor the type of information stored therein." No. C09-0642RSL, 2011 WL 887731, at *8 (W.D. Wash. Mar. 10, 2011), modified on other grounds on reconsideration, 2011 WL 1900140 (May 19, 2011). Far from it, the user manuals would reveal, among other things, "step-by-step instructions" on how to retrieve the information in the TECS and ATS databases, "specific drop down menus

and instructions for querying and navigating the database," "names of specific modules" within the databases, "instructions on how to read results screens, system capabilities with respect to records that would reveal law enforcement techniques, and information about querying abilities and results that would reveal capabilities of system." Suzuki Decl. ¶ 40.

Release of that information could reasonably be expected to risk circumvention of the law because it "would facilitate unlawful access to law enforcement databases and disclose precise procedures followed by CBP officers when conducting law enforcement queries to determine the admissibility of international travelers and would disclose scope of investigations and techniques/procedures for border law enforcement and investigations, thereby risking circumvention of the law." Id. Those risks of circumvention (for instance, through the disclosure of procedures followed by CBP officers and the disclosure of scope of investigations and techniques/procedures for border law enforcement and investigations) do not necessarily depend on hacking as a precondition as plaintiff suggests. Furthermore, release of the information in the user manuals could facilitate hacking in and of itself: "This information would instantly aid a hacker with valuable information on the structure, pattern and sequence of the law enforcement queries ***facilitating both unauthorized access to and utilization of the system***." Supp. Suzuki Decl. ¶ 18 (emphasis added).

The reality of hackers poses additional, significant risks of circumventing the law. In her supplemental declaration, Suzuki has added a wealth of further factual information showing why release of the user guides could risk circumvention of the law by hackers. See id. ¶¶ 17-19, 22. To list only a few items:

> Such disclosure could enable unauthorized users to gain access to the agency's law enforcement databases and alter, add, or delete information altogether, or alter an individual's patterned behaviors under surveillance, thus destroying the integrity of an investigation. . . . The disclosure of internal operating systems that identify certain parameters or functions within the databases could further enable such unauthorized users to disrupt or destroy the systems at worst; or to evade detection and or make unauthorized changes to law enforcement records which could go unnoticed and become permanent. In addition, if the system were to be hacked it would put at risk ongoing investigations, including the exposure of informants, witnesses and other highly sensitive information that could lead to intimidation of witnesses, destruction of evidence and other actions designed to thwart investigative and law enforcement activities.

Supp. Suzuki Decl. ¶ 17. The risk of circumvention would not be limited to CBP: "Because of the interconnectivity between the agency's law enforcement databases and those of other agencies, such distortion of the information contained in the database could have far-reaching effects and could impair other agencies' law enforcement operations or missions." Id.

Plaintiff fails to address the reality of hacking in the present day, but that does not mean it does not exist. This court may take judicial notice that hacking and unauthorized systems access are real and important problems afflicting large organizations in the United States and around the world (for instance, the recent cases of voicemail hacking by News of the World, computer network hacking at Sony and email hacking at Google). Against the backdrop of the real and significant problem of hacking, it is clear that release of the user manuals "could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E).

Importantly, the statutory language "could reasonably be expected to risk circumvention of the law" does not set an onerous bar:

> In short, the exemption looks not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk.

Mayer Brown LLP v. IRS, 562 F.3d 1190, 1193 (D.C. Cir. 2009). This is true even if FOIA exemptions in general should be narrowly construed. See id. at 1194 ("But broad language – even when construed narrowly – is broad language.").

Of particular relevance here, "Exemption 7(E) clearly protects information that would *train* potential violators to evade the law or *instruct* them how to break the law. But it goes further. It exempts from disclosure information that could *increase the risks* that a law will be violated or that past violators will escape legal consequences." Id. (italics in original). The TECS and ATS user manuals literally provide training and instructions that could be used to evade or break the law or, at a minimum, could increase the risks that a law will be violated or that past violators will escape legal consequences. It also "could encourage decisions to violate the law or evade punishment." Id. at 1193.

In closing, Suzuki's detailed explanations in her original and supplementary declarations

"provide non-conclusory reasons why disclosure of each category of withheld documents risk circumvention of the law." Feshbach v. SEC, 5 F. SUPP.2d 774, 787 (N.D. Cal. 1997) (citing PHE, Inc. v. U.S. Dep't of Justice, 983 F.2d 248, 252 (D.C. Cir. 1993)). Those detailed explanations go far beyond the conclusory statement rejected in Feshbach. Cf. Feshbach, 5 F. Supp. 2d at 786-87 (rejecting as conclusory the offered explanation, "regarding only one of many categories of documents withheld pursuant to exemption 7(E)," that the documents would "reveal Commission law enforcement procedures, techniques, and strategies, the disclosure of which could be used to circumvent federal securities law"). Because "the substance of the withheld information is clear from the descriptions in the affidavit" and because "[t]he affidavit also demonstrates logically how the release of that information might create a risk of circumvention of the law," CBP has met the risk-of-circumvention requirement. PHE, Inc., 983 F.2d at 251 (holding that information from an FBI manual was covered by Exemption 7(E)); see also Mayer Brown LLP, 562 F.3d at 1196 (holding that IRS settlement guidelines were covered by Exemption 7(E)).

3. Exemption 7(E) Applies Notwithstanding FOIA Subsection (a)(2)(C).

FOIA provides that an agency "shall make available... (C) administrative staff manuals and instructions to staff that affect a member of the public." 5 U.S.C. § 552(a)(2)(C). Plaintiff's attempt to portray the TECS and ATS user guides as nothing more than "administrative staff manuals" required to be released under subsection (a)(2)(C) is off target. First, the disclosure provision of subsection (a)(2)(C) does not cover material that otherwise falls within one of FOIA's enumerated exemptions such as Exemption 7(E). See Windels, Marx, Davies & Ives v. Dep't of Commerce, 576 F. SUPP. 405, 411 (D.D.C. 1983) (stating that because the requested information "is specifically exempted by Exemption[ ]... 7, disclosure cannot be required by § 552(a)(2)(C) since the provision 'does not apply' to any material which falls within one of FOIA's exemptions").

Second, the TECS and ATS user guides do not fall under § 552(a)(2)(C) in any event. That section applies to "an agency's substantive or procedural law" when disclosure of such information "serves the very goals of law enforcement by encouraging knowledgeable and

voluntary compliance with the law." Hawkes v. IRS, 467 F.2d 787, 795 (6th Cir. 1972). This includes manuals and instructions that provide "criteria for investigative action[,] standards for evaluation and so forth." Id.; see also PHE, Inc., 983 F.2d at 251 (requiring disclosure of manuals "containing the discussion of search and seizure law and the digest of useful caselaw" as "precisely the type of information appropriate for release under the FOIA").

The ATS and TECS user guides do not contain that kind of information. Instead, they provide in-depth, step-by-step guides for navigating and using sensitive law-enforcement databases. Suzuki Decl. ¶ 40. The user guides are "extraordinarily detailed instruction manuals" which contain, for example, "detailed keystroke by keystroke instructions on how to perform a query that reveals the structure of the law enforcement systems." Supp. Suzuki Decl. ¶ 19. The "staff manuals and instructions" disclosure requirement of § 552(a)(2)(C) does not cover this kind of detailed, technical information. See Windels, 576 F. SUPP. at 411 (holding that computer program instructions on isolating and analyzing relevant data need not be disclosed under § 552(a)(2)(C)).

4. The Privacy Act Does Not Require Release of the User Guides.

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). Plaintiff argues that this requirement covering policies and practices somehow extends to the detailed technical information contained in the TECS and ATS user guides. That argument is without merit.

First, CBP fulfilled its obligations under Privacy Act subsection (e)(4)(E) by making the required information available in its SORNs for the relevant record systems. See 73 FR 77778, 77780-82 (Dec. 19, 2008) (TECS SORN detailing the database location, covered individuals, categories of records, purpose, routine uses, and "policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system"); 72 FR 43650, 43653-55 (Aug. 6, 2007) (ATS SORN detailing the same information). Second, plaintiff has cited not a single case supporting his farfetched proposition that the "policies and practices of the agency regarding storage, retrievability, [and] access controls," Pl.'s MSJ at 13:5-6, somehow extend to detailed,

step-by-step instructions contained in user manuals. It is self-evident that instructions are not policies and practices; they are instructions. It defies logic to suggest that the Privacy Act was intended to bloat the Federal Register by requiring federal agencies to publish all of their database user manuals as part of their SORNs.

Plaintiff's reliance on Doe v. General Services Administration, 544 F. Supp. 30, 536-37 (D. Md. 1982), is misplaced. The "Release and Access Guide" at issue in Doe did not consist of the type of step-by-step instructions contained in the TECS and ATS user manuals, but rather set forth "agency interpretations of the Privacy Act." Doe, 544 F. Supp. at 537. Moreover, the parties in Doe were not litigating the disclosure of the Release and Access Guide, nor was the status of that guide firmly resolved. See id. at 536 ("Although it is not altogether certain, it appears that the Release and Access Guide is a statement of agency 'policies and procedures' regarding 'retrievability, access controls, retention, and disposal of records.'" (citing 5 U.S.C. §552a(e)(4)(E)).

5. CBP Has Met FOIA's Segregability Requirement.

"The burden is on the agency to establish that all reasonably segregable portions of a document have been segregated and disclosed." Pac. Fisheries Inc. v. United States, 539 F.3d 1143, 1148 (9th Cir. 2008) (citing 5 U.S.C. § 552(a)(4)(B), (b)). In Pl.'s MSJ, plaintiff does not dispute that "[t]he agency need not disclose non-exempt portions of a document if 'they are inextricably intertwined with exempt portions such that the excision of exempt information would impose significant costs on the agency and produce an edited document with little informational value.'" Def.'s MSJ at 17:25-28 (citing Willamette Indus., Inc. v. United States, 689 F.2d 865, 867-68 (9th Cir. 1982)). Nor does plaintiff dispute that CBP, in justifying its claim of nonsegregability, "'is not required to provide so much detail that the exempt material would be effectively disclosed.'" Def.'s MSJ at 18:2-3 (citing Johnson v. Exec. Office for U.S. Attorneys, 310 F.3d 771, 776 (D.C. Cir. 2002)). Instead, CBP must simply support its claim of nonsegregability with "'reasonable specificity.'" Def.'s MSJ at 18:4-5 (citing Johnson, 310 F.3d at 776.

Plaintiff argues that the Suzuki Decl. was insufficient for CBP to meet its burden.[1] CBP disagrees, but believes that the Supp. Suzuki Decl. addresses any outstanding concerns that the plaintiff may have raised. Suzuki explained that "both Users' Guides discuss in detail and in conjunction with the operation of the data systems the observations, assessments, methodologies, programs and capabilities of those systems, all of which are inextricably intertwined with the instructions to the user." Supp. Suzuki Decl. ¶ 17.

Suzuki further elaborated that segregation would require a large amount of effort resulting in meaningless words or phrases amounting to less than 2 percent of each page:

> Even knowing when to click on an icon versus when to select a drop down menu or when to enter information would reveal how CBP officers use the system to search for information. . . . After deleting both the navigational information (*e.g.*, "click", "select", "enter", etc.) and the substantive information ("find", "port", "secondary referrals", "arrivals", etc.), in order to protect how CBP performs its searches, all that would be left would be meaningless words or phrases ("the", "choose", "perform the following"). It is estimated that such information would be less than 2 percent of each page. It would also require a large amount of effort to parse out these words dispersed throughout the page and would only result in unintelligible gibberish.

Supp. Suzuki Decl. ¶ 18.

Accordingly, following her "page-by-page, line-by-line review," Suzuki concluded that "no portions can be segregated and disclosed. The few non-exempt words and phrases that are dispersed throughout the records withheld in full, if disclosed, would be meaningless and would not serve the purpose of FOIA–to open agency action to the light of public scrutiny." Id. ¶ 26; see also id. ¶ 25 (explaining that the withheld information "is so intertwined with protected material that segregation is not possible or its release would have revealed the underlying protected material").

In Johnson, the court held that the agency met its obligation regarding segregability when it submitted, in combination with its Vaughn index, an affidavit in which the affiant explained that she had "personally conducted a line-by-line review of each document withheld in full and

---

[1] Plaintiff purported to quote CBP's justification "in full," but quoted only part of one paragraph of the justification. See Pl.'s MSJ at 12 n.16 (quoting part of Suzuki Decl. ¶ 42). In fact, Suzuki devoted two paragraphs in her declaration to segregability. Suzuki Decl. ¶¶ 41, 42.

determined that 'no documents contained releasable information which could be reasonably segregated from the nonreleasable portions.'" 310 F.3d at 776; see also Nat'l Sec. Archive Fund, Inc. v. CIA, 402 F. Supp. 2d 211, 221 (D.D.C. 2005) (holding that the segregability requirement was met when the agency's declaration, taken in its entirety, showed that "those isolated words or phrases that might not be redacted for release would be meaningless"). Likewise here, the detailed information presented in the Supp. Suzuki Decl., along with the detailed Vaughn Index and the information in the Suzuki Decl., meets CBP's "obligation to show with 'reasonable specificity' why a document cannot be further segregated."[2] Johnson, 310 F.3d at 776.

B. CBP Properly Withheld Information Under the Privacy Act.

In Pl.'s MSJ, plaintiff does not contest the redaction of third-parties' personally identifying information ("PII") on 24 pages of PNR data released by the Privacy Branch. See generally Def.'s MSJ (Doc. #31) at 19:14-20:5. Thus, for Privacy Act purposes, plaintiff challenges only the withholding of records under Privacy Act Exemptions (j)(2) and (k)(2), 5 U.S.C. §§ 552a(j)(2), (k)(2). Importantly, plaintiff does not dispute that, substantively, the final rule that was enacted does exempt the records at issue. See 6 C.F.R. Pt. 5, App. C, ¶ 45. Instead, plaintiff makes two procedural arguments: (1) that CBP cannot rely on the SORN because it was not a final rule, and

---

[2] Plaintiff suggests as possible relief that the court should "conduct its own *in camera* review of the user guides." Pl.'s MSJ at 12:9. But plaintiff has not addressed, much less established, the four factors he contends are required for *in camera* review: "(1) judicial economy; (2) actual agency bad faith; (3) strong public interest; and (4) the parties' request for *in camera* review." Id. at 11 n.15 (citing Hiken v. Dep't of Defense, 521 F. Supp. 2d 1047, 1056 (N.D. Cal. 2007)). CBP notes that Hiken borrowed these four factors from the Sixth Circuit, which of course does not bind this court. See id. (citing Jones v. FBI, 41 F.3d 238 (6th Cir.1994)). CBP does not concede that this is the test, and in the absence of any application of the Hiken factors by plaintiff to the facts of this case, and in the absence of any analysis by plaintiff of *in camera* review in general, CBP requests that, if the court is inclined to further explore the possibility of *in camera* review, CBP be permitted to address the subject in supplemental briefing and/or at the hearing. CBP simply notes here, respectively as to each Hiken factor, that: (1) plaintiff has failed to show any judicial economy, and *in camera* review by its very nature requires court resources; (2) there is no allegation or showing of agency bad faith; (3) plaintiff has failed to establish a strong, if any, public interest; and (4) CBP has not requested *in camera* review. CBP also believes that its declarations and Vaughn Index are sufficiently detailed to establish that all of the information at issue was properly withheld.

(2) that the final rule should not be applied retroactively. Those arguments miss the mark.

First, CBP depends on the final rule, not on the SORN, for the claimed exemptions. CBP expressly stated in Def.'s MSJ that "CBP promulgated a rule" exempting the information at issue and cited to the final rule; it also cited the SORN as part of a "see also" cite. Def.'s MSJ at 21:18-23. CBP also said that it "stated the reasons ***in the rule itself*** why the system of records is to be exempt from the Privacy Act's access provisions," id. at 21:24 (emphasis added), and cited the final rule in quoting those reasons, id. at 21:25-22:5.[3]

Second, no retroactivity problem is raised by the fact that the final rule regarding the ATS (and BCIS) exemptions was not in place until February 3, 2010. The Privacy Act says, "Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975." 5 U.S.C. § 552a(g)(5). It does not mention whether retroactivity is permitted after September 27, 1975.

To the extent the Privacy Act does not speak directly to the question at issue, there is a "general rule" that "'a court should apply the law in effect at the time it renders its decision.'" Southwest Ctr. for Biological Diversity v. U.S. Dep't of Agric., 314 F.3d 1060, 1061 (9th Cir. 2002) (quoting Landgraf v. USI Film Products, 511 U.S. 244, 273 (1994)). Although this "general rule . . . coexists with a presumption against statutory retroactivity," Southwest Ctr., 314 F.3d at 1061, the Ninth Circuit has held that there is no impermissible retroactive effect when a FOIA exemption is invoked that was created after a request but before the resolution of a lawsuit.[4] See id. at 1062. In Southwest Ctr., the plaintiff filed a FOIA request regarding certain data about a rare bird. See id. at 1061. When the plaintiff did not receive a response, it filed suit in district court. See id. While the action was pending, Congress passed the 1998 Parks Act, § 207 of which the

---

[3] The final rule also stated the reasons for exempting BCIS records. See 6 C.F.R. Pt. 5, App. C, ¶ 46.

[4] Although Southwest Ctr. involved a FOIA exemption, its reasoning applies equally well to Privacy Act exemptions, especially given that FOIA standards are often applied to the Privacy Act. Cf. Lane, 523 F.3d at 1139 n.9 (holding that the standard governing adequacy of search under FOIA also governs adequacy of search under the Privacy Act).

district court held precluded the release of the requested data. See id. On appeal, the plaintiff argued that § 207 could not be applied to an action that was already pending when § 207 was enacted. See id.

Finding no expression of Congressional intent to guide it, the Ninth Circuit applied the factors set forth by the Supreme Court in Landgraf, specifically whether retroactive effect "would 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 1062. The Ninth Circuit rejected the plaintiff's argument that retroactive application of § 207 impaired a right to the information the plaintiff possessed when it filed suit or when it made its earlier request. See id. The court explained that "the 'action' of the [plaintiff] was merely to request or sue for information; it was not to take a position in reliance upon existing law that would prejudice the [plaintiff] when that law was changed." Id. (footnote and citations omitted). The court therefore held that there was "no impermissible retroactive effect upon the [plaintiff." Id. The court further noted that application of the exemption furthered Congress's intent to protect the information at issue. See id.

The same reasoning applies here. Like the plaintiff in Southwest Ctr., Hasbrouck's action was merely to request information; he did not take a position in reliance upon existing law that would prejudice him once the final rule was enacted. If anything, Hasbrouck's situation is even less tenable than the plaintiff's in Southwest Ctr. because in that case, the new law was passed after the plaintiff had already filed suit in district court. Here, the final rule of February 3, 2010, was promulgated more than six months before Hasbrouck filed his complaint (Doc. #1) on August 25, 2010. Moreover, the ATS SORN containing the proposed exemptions was published on August 6, 2007, three years before Hasbrouck filed suit. See Notice of Privacy Act System of Records, 72 FR 43650, 43656 (Aug. 6, 2007). Application of the exemption would also further the agency's intent to exempt the materials from access. Thus, there is no impermissible

retroactive effect.[5]

C. CBP Conducted Adequate Searches Under FOIA and the Privacy Act.

1. The Declarations Contain Specific and Detailed Information Sufficient to Establish Adequacy of Search.

Plaintiff, citing two out-of-circuit cases, enumerates six factors which he contends "must" be included in a declaration to establish adequacy of search. See Pl.'s MSJ at 17:16-26. But he cites no Ninth Circuit (or Supreme Court) case holding that those six factors "must" be included. Instead, the Ninth Circuit has adopted a flexible approach and simply requires that affidavits describing agency search procedures be "relatively detailed in their description of the files searched and the search procedures" and be "nonconclusory and not impugned by evidence of bad faith." Zemansky v. EPA, 767 F.2d 569, 573 (9th Cir. 1985). This flexible approach comports with the Ninth Circuit's pronouncement that "[t]he adequacy of the search . . . is judged by a standard of reasonableness and depends, not surprisingly, upon the facts of each case." Id. at 571.

As there is no evidence or allegation of bad faith, the only question is whether the declarations are "relatively detailed in their description of the files searched and the search procedures" and are "nonconclusory." Id. at 573. As seen below, the original and supplemental declarations of Suzuki and Castelli meet this standard. In fact, they cover the six factors plaintiff says "must" be included and more.

The declarations contained, among other things, the following information:

(1): The systems searched. See Suzuki Decl. ¶¶ 8, 16, 19, 22, 24, 25; Supp. Suzuki Decl. ¶¶ 6, Castelli Decl. ¶ 13; Supp. Castelli Decl. ¶ 5.

(2): Why the systems searched were the only ones reasonably likely to contain responsive records. See Suzuki Decl. ¶¶ 18-20; Supp. Suzuki Decl. ¶¶ 11-14, 20; Supp. Castelli Decl. ¶¶ 3, 5.

---

[5] By way of comparison, if the court were to adopt plaintiff's reasoning, then CBP could still rely on FOIA Exemption (b)(2), 5 U.S.C. § 552(b)(2), since the Supreme Court did not issue its decision in Milner v. Dep't of the Navy, – U.S. –, 131 S. Ct. 1259 (Mar. 7, 2011), concerning that exemption until 2011– after plaintiff made his requests in 2007 and 2009 and after plaintiff filed this suit in 2010. See generally Def.'s MSJ at 3 n.6.

(3): The search terms used, as well as why certain search terms were not used. See Suzuki Decl. ¶ 16, 22, 24, 25; Supp. Suzuki Decl. ¶¶ 7, 8; Castelli Decl. ¶ 13; Supp. Castelli Decl. ¶¶ 6-10.

(4): How the searches were conducted, as well as the process for reviewing responsive documents and the coordination between the FAPL Branch, FOIA Division, Privacy Act Policies and Procedures Branch and the Passenger Branch. See Suzuki Decl. ¶¶ 16, 22, 24, 25; Supp. Suzuki Decl. ¶¶ 7-9; Castelli Decl. ¶ 13; Supp. Castelli Decl. ¶¶ 5-11.

(5): The individuals responsible for the searches. See Suzuki Decl. ¶¶ 8, 16, 19, 22; Supp. Suzuki Decl. ¶¶ 7, 13, 14; Castelli Decl. ¶¶ 13-14; Supp. Castelli Decl. ¶¶ 6-10.

(6): How long the searches took to perform. See Supp. Suzuki Decl. ¶ 6; Supp. Castelli Decl. ¶ 11.

Thus, CBP's declarations were sufficiently detailed and nonconclusory. Cf. Lane, 523 F.3d at 1139 (holding that affidavit was sufficiently detailed when it explained the search procedures used, staff members contacted, files examined, time spent on searches, and review of responsive documents).

2. The Search for Records Under FOIA Was Adequate.

Plaintiff contends that the FOIA Branch did not search for records in the correct places and did not use the proper search parameters. These contentions are without merit.

First, CBP searched for records in the correct places. Plaintiff complains that CBP did not explain how its records are stored. But "[b]y explaining the systems that were searched, CBP did explain how the records are stored." Supp. Suzuki Decl. ¶ 21. CBP explained how it searched TECS for BCI, API and information on primary and secondary processing; explained how it searched ATS for PNR; referenced the SORNs which detail the information that is kept in each system; and explained that it searched for information covered by each of the SORNs for TECS, BCI, APIS and ATS. Id. CBP "searched every possible repository likely to maintain responsive records." Id.

Second, CBP used the correct search parameters. Based on Suzuki's experience, CBP is most likely to retrieve all responsive records about an individual by searching on the individual's first name, last name and date of birth . Id. ¶ 8. That was indeed the case here, as a search using plaintiff's first name, last name and date of birth turned up the records that plaintiff appeared to be seeking. Id. Thus, although plaintiff lists various search terms that he says should have been used, there was no need to use those additional terms. Suzuki explained in detail why it was not necessary to search using plaintiff's middle name or using misspellings, similar pronunciations or transpositions. Id.

The search for responsive FOIA records took approximately 10 hours. Id. ¶ 6.

3. The Search for Records Under the Privacy Act Was Adequate.

CBP also conducted a reasonable search for records under the Privacy Act. It was reasonable for CBP to search for PNR records in the module where that data is collected and maintained, as Castelli explained: "Plaintiff requested PNR (Passenger Name Record) records, and CBP queried the ATS-P (ATS-Passenger) module, which collects and maintains the PNR data that is provided to airlines and travel agents by or on behalf of passengers seeking to book travel into or out of the United States." Supp. Castelli Decl. ¶ 5. In addition to the detailed information contained in the original Castelli Decl. ¶¶ 11-14, Castelli in his supplemental declaration has provided more details about the various queries and searches that were conducted. See Supp. Castelli Decl. ¶¶ 6-11. For instance, Castelli (1) explained that the Chief of the Passenger Branch "used all of the search terms that were specifically identified by the Plaintiff in his appeal letter dated September 17, 2007, in the four specific search combinations he specifically requested," id. ¶ 8; (2) provided detailed information about the "'back-end' search, or more intensive technical extraction from the underlying data tables for the ATS-P database," that was conducted, id. ¶ 9; and (3) provided detailed information about the manual search, retrieval and review that the Chief of the Passenger Branch conducted of the ATS-P end user interface, id. ¶ 10. He explained why there were unlikely to be misspellings of plaintiff's name, but that any such misspellings nevertheless would have been uncovered during the manual review. Id. Indeed, there were no such records. Id.

The technical extraction process took 8 days to complete and the manual review of each record and compilation of data took 6 hours. Id. ¶ 11.

4. CBP Adequately Searched for Records Despite Plaintiff's Belief That Other Records Should Exist.

Finally, plaintiff lists certain records that he believes should exist. "[T]he issue to be resolved is not whether there might exist any other documents possibly responsive to the request, but whether the *search* for those documents was *adequate*." Zemansky, 767 F.2d at 571 (italics in original).

Regarding, plaintiff's belief that there should be various email communications, Suzuki explained that she worked approximately 40 feet from Castelli at the time in question. Supp. Suzuki Decl. ¶ 9. She also explained that records of communications with DHS personnel lie beyond the access and authority of CBP to search for or disclose, and must be requested from DHS. Id. ¶ 12. Castelli explained that the email record system "is exempt from the access provision of the Privacy Act and likely would also be withheld pursuant to exemption 2 of the FOIA relating to internal matters of a relatively trivial nature." Supp. Castelli Decl. ¶ 3. Email records "likely would also be withheld pursuant to the deliberative process privilege as applied under [FOIA]." Id. ¶ 13. Castelli also explained that certain email correspondence plaintiff refers to "was neither requested in the Plaintiff's Privacy Act Appeal, dated September 13, 2007, nor responsive to that request. Id.

As to the weekly list of "significant FOIA activities" plaintiff mentions, Suzuki explained that plaintiff's three initial requests in 2009 and plaintiff's appeals were not reported as significant. Supp. Suzuki Decl. ¶ 10. Suzuki also explained that Plaintiff's 2007 request was unlikely to be reported as significant due to its nature and that the appeal was not covered by the reporting requirement because it was handled as a Privacy Act appeal. Id. Castelli explained that the weekly report does not apply to Privacy Act appeals and that plaintiff's Privacy Act appeal was not reported. Supp. Castelli Decl. ¶ 14.

As to access logs, Suzuki explained that they are not used to generate reports to memorialize search terms used and therefore would not be responsive. Supp. Suzuki Decl. ¶ 11.

Castelli explained that the Privacy Branch did not search for audit records because they were neither requested nor responsive. Supp. Castelli Decl. ¶ 15. Moreover, audit records are exempt from access under Privacy Act Exemptions (j)(2) and (k)(2). Id.

Suzuki explained that telephone logs do not exist. Supp. Suzuki Decl. ¶ 12. Regarding Stephen Christenson, it was reasonable and adequate for Suzuki to check the employee directory and the mailroom. Again, "the issue to be resolved is not whether there might exist any other documents possibly responsive to the request, but whether the *search* for those documents was *adequate*." Zemansky, 767 F.2d at 571 (italics in original). Finally, software specifications were not searched because they would not explain how to retrieve information from the system and were not responsive. Id. ¶¶ 13, 14.

IV. CONCLUSION.

For the foregoing reasons, the court should grant defendant's motion for summary judgment (Doc. #31) and deny plaintiff's cross-motion for summary judgment (Doc. #37).

Dated: July 15, 2011

Respectfully submitted,

MELINDA HAAG
United States Attorney

/s/
NEILL T. TSENG
Assistant United States Attorney