

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

<b>ELECTRONIC FRONTIER FOUNDATION</b>	)	
	)	
Plaintiff,	)	<b>Consolidated Cases</b>
	)	
v.	)	Civil Action No. 06-1988 (ESH)
	)	
<b>DEPARTMENT OF HOMELAND SECURITY</b>	)	Civil Action No. 06-2154 (RBW)
	)	
Defendant.	)	
_____	)	

**DEFENDANT’S MOTION FOR PARTIAL SUMMARY JUDGMENT**

Pursuant to Rule 56 of the Federal Rules of Civil Procedure, defendant Department of Homeland Security respectfully moves for partial summary judgment on the issue of plaintiff’s entitlement to expedited processing of requests submitted to defendant pursuant to the Freedom of Information Act, 5 U.S.C. § 552. In support of its motion, defendant submits the accompanying memorandum of points and authorities and statement of material facts.

Respectfully Submitted,

Dated February 22, 2007

PETER D. KEISLER  
Assistant Attorney General

JEFFREY A. TAYLOR  
United States Attorney

ELIZABETH J. SHAPIRO  
(D.C. Bar 418925)  
Assistant Branch Director  
U.S. Department of Justice  
Civil Division, Federal Programs Branch

/s/ John R. Coleman  
JOHN R. COLEMAN  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch

Mailing Address

P.O. Box 883  
Washington, D.C., 20044

Delivery Address

20 Massachusetts Avenue, NW, Room 6118  
Washington, D.C. 20530  
Telephone: (202) 514-4505  
Facsimile: (202) 616-8187  
john.coleman3@usdoj.gov

/s/ Adam D Kirschner

ADAM D. KIRSCHNER  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch

Mailing Address

P.O. Box 883  
Washington, D.C., 20044

Delivery Address

20 Massachusetts Avenue, NW, Room 7126  
Washington, D.C. 20530  
Telephone: (202) 353-9265  
Fax: (202) 616-8470  
adam.kirschner@usdoj.gov

Counsel for Defendant

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

<b>ELECTRONIC FRONTIER FOUNDATION</b>	)	
	)	
Plaintiff,	)	<b>Consolidated Cases</b>
	)	
v.	)	Civil Action No. 06-1988 (ESH)
	)	
<b>DEPARTMENT OF HOMELAND SECURITY</b>	)	Civil Action No. 06-2154 (RBW)
	)	
Defendant.	)	
	)	

---

**DEFENDANT’S MEMORANDUM IN SUPPORT OF ITS MOTION FOR PARTIAL  
SUMMARY JUDGMENT AND IN OPPOSITION TO  
PLAINTIFF’S MOTION FOR PARTIAL SUMMARY JUDGMENT**

Plaintiff, the Electronic Frontier Foundation (“EFF”), has filed two separate lawsuits against the Department of Homeland Security (“DHS”) challenging, *inter alia*, DHS’s denial of plaintiff’s requests to expedite processing of its Freedom of Information Act (“FOIA”) requests. This Court has consolidated these two lawsuits for the sole purpose of deciding the expedition issue.

The general rule is that FOIA requests are processed in the order they are received. When Congress amended FOIA to provide for expedited processing of certain FOIA requests, it made clear that expedited processing should be granted only in narrow circumstances because an expedited FOIA request, by jumping to the front of the processing queue, necessarily prejudices all prior requesters who have not sought such special treatment. By requesting expedited processing of the requests at issue in this case, plaintiff is attempting to broaden this very narrow exception to the general rule.

Plaintiff is not entitled to expedited processing of the FOIA requests involved in these

consolidated cases because plaintiff fails to meet either of the two necessary preconditions a requestor must satisfy to be entitled to expedited processing. In each case, plaintiff has failed to demonstrate that it is primarily engaged in disseminating information, the precondition for expedited processing. In fact, as revealed by plaintiff's own website, plaintiff is primarily involved in litigation—not disseminating information. Furthermore, plaintiff has failed to demonstrate that there is an urgency to inform the American public about the subject matter of either request. In addition to these deficiencies, plaintiff has also failed to administratively appeal the denial of two of its requests for expedited processing before bringing suit. Plaintiff's failure to exhaust its administrative remedies deprives this Court of subject matter jurisdiction over the claim for expedition of these requests.

## **BACKGROUND**

### **A. Statutory and Regulatory Framework**

#### **1. The 1996 FOIA Amendments**

Agencies ordinarily process FOIA requests for agency records on a first-in, first-out basis. In 1996, Congress amended the FOIA to provide for “expedited processing” of certain categories of requests. See Electronic Freedom of Information Act Amendments of 1996, Pub. L. 104-231, § 8 (codified at 5 U.S.C. § 552(a)(6)(E)) (“E-FOIA”). Expedition, when granted, is an exceptional process that entitles requestors to move immediately to the front of an agency processing queue, ahead of requests filed previously by other persons.

As part of E-FOIA, Congress directed agencies to promulgate regulations providing for expedited processing of requests for records. Specifically, Congress directed agencies to enact regulations providing for expedited processing (i) “in cases in which the person requesting the

records demonstrates a compelling need,” 5 U.S.C. § 552(a)(6)(E)(i)(I), and (ii) “in other cases determined by the agency.” Id. § 552(a)(6)(E)(i)(II). The statute defines “compelling need” to mean:

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

Id. § 552(a)(6)(E)(v)(I), (II). FOIA requests granted expedited processing are to be processed “as soon as practicable.” Id. § 552(a)(6)(E)(iii).

The E-FOIA House Report, upon which the D.C. Circuit has relied in construing the amendments, states that the E-FOIA expedition categories should be “narrowly applied.” Al-Fayed v. Central Intelligence Agency, 254 F.3d 300, 310 (D.C. Cir. 2001) (quoting Electronic Freedom of Information Act Amendments of 1996, H.R. Rep. No. 104-795, at 26 (1996)). As the Court of Appeals explained in Al-Fayed: “Congress’ rationale for a narrow application is clear: ‘Given the finite resources generally available for fulfilling FOIA requests, unduly generous use of the expedited processing procedure would unfairly disadvantage other requestors who do not qualify for its treatment.’ . . . Indeed, an unduly generous approach would also disadvantage those requestors who do qualify for expedition, because prioritizing all requests would effectively prioritize none.” 254 F.3d at 310 (quoting H.R. Rep. No. 104-795, at 26).

The requestor bears the burden of showing that expedition is appropriate. See Al-Fayed, 254 F.3d at 305 n.4 (quoting H.R. Rep. No. 104-795, at 25). Agency decisions to deny or affirm

denial of a request for expedited processing are subject to judicial review. 5 U.S.C.

§ 552(a)(6)(E)(iii). Such judicial review “shall be based on the record before the agency at the time of the determination.” Id.

The standard for reviewing agency decisions to deny expedition depends on the ground for decision. As noted above, an agency may grant expedition “in cases in which the person requesting the records demonstrates a compelling need,” 5 U.S.C. § 552(a)(6)(E)(i)(I), or “in other cases determined by the agency.” 5 U.S.C. § 552(a)(6)(E)(i)(II); see also Al-Fayed, 254 F.3d at 307 n.7 (noting this latter provision gives agencies “‘latitude to expand the criteria for expedited access’ beyond cases of ‘compelling need’”) (quoting H.R. Rep. No. 104-795, at 26). A decision denying expedited processing for failure to establish “compelling need” under Section 552(a)(6)(E)(i)(I) is reviewed *de novo*. See Al-Fayed, 254 F.3d at 308. A decision denying expedited processing for failure to meet criteria established by an agency under Section 552(a)(6)(E)(i)(II) is reviewed under a more deferential “reasonableness” standard. See Al-Fayed, 254 F.3d at 307 n.7 (noting that, “to the extent [the agency FOIA] regulations expand the criteria for expedited processing beyond ‘compelling need,’ the agencies reasonably determined that plaintiffs’ requests did not meet the expanded criteria”).

## **2. Department of Homeland Security Regulations**

DHS implemented E-FOIA by final rule effective January 27, 2003. See Freedom of Information Act and Privacy Act Procedures, 68 Fed. Reg. 4,056 (January 27, 2003) (codified at 6 C.F.R. §§ 5.1-5.12). This rule, which governs FOIA requests directed to DHS and its components (see 6 C.F.R. § 5.1), states that “[r]equests and appeals will be taken out of order and given expedited treatment whenever it is determined that they involve:”

- (i) Circumstances in which the lack of expedited treatment could reasonably be expected to pose an imminent threat to the life or physical safety of an individual;
- (ii) An urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information.

6 C.F.R. § 5.5(d)(1). Thus, these regulatory provisions implement the statutory “compelling need” standard. See 5 U.S.C. § 552(a)(6)(E)(v). Any “request for expedited processing must be submitted to the component that maintains the record requested.” 6 C.F.R. § 5.5(d)(2). If the “request for expedited processing is denied, any appeal of that decision shall be acted on expeditiously.” 6 C.F.R. § 5.5(d)(4).

As Congress recognized, agency expedition decisions depend on “factual and subjective judgments about the circumstances cited by requestors to qualify them for ‘expedited processing.’” H.R. Rep. No. 104-795, at 26. Accordingly, DHS requires requestors to “explain[] in detail the basis for” their expedition requests. 5 C.F.R. § 5.5(d)(3); see also H.R. Rep. No. 104-795, at 26 (“the requestors will need to explain in detail their basis for seeking such treatment”). For requests based on an urgency to inform the American public (category (ii) above), the requestor “must establish a particular urgency to inform the public about the government activity involved in the request, beyond the public’s right to know about government activity generally.” Id.; see also H.R. Rep. No. 104-795, at 26. A requestor within category (ii) who is not a full-time member of the news media must establish that he or she “is a person whose main professional activity or occupation is information dissemination, though it need not be his or her sole occupation.” 5 C.F.R. § 5.5(d)(3).

**B. Plaintiff's Requests for Expedited Processing**

This litigation concerns two separate challenges to DHS's denials of plaintiff's requests for expedited processing. Civil Action No. 06-1988 (ESH) involves plaintiff's request for expedited processing of documents relating to the negotiation of the Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record Data ("Interim Agreement"). See October 20, 2006 letter from EFF to DHS ("Interim Agreement Request") (attached as Exhibit A to plaintiff's motion for partial summary judgment). Civil Action No. 06-2154 (RBW) involves two requests for expedited processing of documents relating to the Automated Targeting System ("ATS"). See November 7, 2006 letter from EFF to DHS ("First ATS Request") (attached as Exhibit E to plaintiff's motion for partial summary judgment); December 6, 2006 letter from EFF to DHS ("Second ATS Request") (attached as Exhibit F to plaintiff's motion for partial summary judgment).

**1. Plaintiff's Interim Agreement Request**

In the aftermath of September 11, 2001, Congress enacted legislation requiring any air carrier operating flights to or from the United States to provide the Customs Service (now part of the Bureau of Customs and Border Protection ("CBP"))<sup>1</sup> with electronic access to Passenger Name Record ("PNR") data. Aviation and Transportation Security Act, Pub. L. No. 107-71, § 115, 115 Stat. 597, 623 (codified at 49 U.S.C. § 44909(c)(3)) ("[C]arriers shall make passenger name record information available to the Customs Service upon request."). PNR data is defined by regulation as information contained on an airline's reservation system that sets forth the

---

<sup>1</sup>Effective March 1, 2003, the United States Customs Service was renamed the United States Bureau of Customs and Border Protection ("CBP"). Homeland Security Act of 2002, Pub.L. No. 107-296, § 1502, 116 Stat. 2135, 2308-09 (2002).

identity and travel plans of passengers traveling to or from the United States.<sup>2</sup> PNR data provided to CBP pursuant to the Aviation Transportation Security Act may be shared with other federal agencies in order to protect national security or as otherwise authorized by law. See 49 U.S.C. § 44909(c)(5); 19 C.F.R. § 122.49d(d).

In 2002, following the publication of the interim regulation implementing this statute, the European Commission (“EC”) advised DHS of a potential conflict between the regulation and European Union (“EU”) law that, in certain circumstances, restricts the cross-border sharing of personal data absent a showing of adequate privacy safeguards.<sup>3</sup> To ensure CBP’s continued access to all PNR data and to address alleged privacy concerns under EU law, the EC and the United States committed to negotiate an amicable resolution of this potential conflict. PNR Privacy Report at 11-12. In the course of these negotiations, CBP issued a set of representations, known as the “Undertakings,” setting forth how CBP would handle PNR data for flights between the U.S. and the EU.<sup>4</sup> On May 17, 2004, the EC announced its conclusion that CBP’s treatment of PNR data pursuant to the Undertakings provided an “adequate level of protection” for the

---

<sup>2</sup>Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or From the United States, 67 Fed. Reg. 42,710, 42,711 (June 25, 2002) (codified as amended at 19 C.F.R. § 122.49d). Thus, PNR data may include: a passenger’s name, intended date of travel, address, payment information, or other itinerary information. 67 Fed. Reg. at 42,711.

<sup>3</sup>DHS Privacy Office, Report Concerning Passenger Name Record Information Derived From Flights Between The U.S. and the European Union, at 11 (Sept. 19, 2005) (hereinafter “PNR Privacy Report”) available at [www.dhs.gov/xlibrary/assets/privacy/privacy\\_pnr\\_rpt\\_09-2005.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_rpt_09-2005.pdf).

<sup>4</sup>See Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41,543, 41,543 (July 9, 2004) (hereinafter the “Undertakings”). The Undertakings were originally issued on May 11, 2004. See 69 Fed. Reg. at 41,543.

privacy of EU citizens under EU law. Undertakings, 69 Fed. Reg. at 41,543. Soon thereafter, the United States and the European Community signed a formal agreement (the “2004 Agreement”) permitting the continued transfer of PNR data to CBP based on the EC’s finding of “adequacy” related to CBP’s commitment to handle the data pursuant to the Undertakings.<sup>5</sup>

On May 30, 2006, the European Court of Justice (“ECJ”) annulled the 2004 Agreement and the related adequacy finding because it concluded they were grounded upon an inapplicable legal basis under EU law.<sup>6</sup> The ECJ did not, however, rule that either the 2004 Agreement or DHS’s handling of PNR data pursuant to the Undertakings infringed rights under EU law. *Id.* at ¶ 61, 70. As a result of this ruling, the United States and the European Union, the competent authority under EU law, began negotiating the agreement, hereinafter referred to as the “Interim Agreement,” that is the subject of plaintiff’s October 20, 2006 request.<sup>7</sup> The Interim Agreement, concluded on October 19, 2006, retained the basic bargain struck in the 2004 Agreement, that—

[i]n reliance upon DHS’s continued implementation of the aforementioned Undertakings *as interpreted in light of subsequent events*, the European Union shall ensure that air carriers operating passenger flights in foreign air transportation to or from the United States of America process PNR data contained in their reservation systems as required by DHS.

Interim Agreement at Art. 1, 72 Fed. Reg. at 349 (emphasis added).

---

<sup>5</sup>See Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (attached as Exhibit 1).

<sup>6</sup>Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Comm’n of the European Communities*, 2006 ECJ CELEX LEXIS 239 at ¶¶ 54-61, 67-70 (May 30, 2006) (attached as Exhibit 2).

<sup>7</sup>See Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, 72 Fed. Reg. 348, 348-49 (Jan. 4, 2007).

The “subsequent events” referred to in this paragraph are certain changes in U.S. law that occurred subsequent to the signing of the 2004 Agreement. These legal developments and their impact on DHS’s implementation of the Undertakings were elucidated in a letter to EU officials that accompanied the Interim Agreement. See 72 Fed. Reg. at 348-51. The letter notes that subsequent to the issuance of the Undertakings in May 2004, Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004, which “required the President to establish an Information Sharing Environment ‘that facilitates the sharing of terrorism information.’”<sup>8</sup> As explained in the letter, “on October 25, 2005, the President issued Executive Order 13,388, directing that DHS and other agencies ‘promptly give access to . . . terrorism information to the head of each other agency that has counterterrorism functions’ and establishing a mechanism for implementing the Information Sharing Environment.” 72 Fed. Reg. at 350 (quoting Exec. Order No. 13,388, 70 Fed. Reg. 62,023, 62,023 (October 25, 2005)).

As permitted by Paragraph 35 of the Undertakings, which states DHS’s intent to “advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings,” the letter advises the EU officials that DHS will interpret the Undertakings in light of these developments and the Undertakings will be “applied so as not to impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating terrorism and related crimes.” 72 Fed. Reg. at 350. Notwithstanding these subsequent events, the EU continues to regard DHS’s handling of

---

<sup>8</sup>Id. at 350; see also Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3665 (2004) (codified at 6 U.S.C. § 485(b)(1)).

PNR data as ensuring an “adequate level of protection” for purposes of EU law.<sup>9</sup>

Plaintiff’s October 20, 2006 FOIA request sought agency records created after May 30, 2006, concerning certain communications from DHS official to EU officials regarding the transfer of PNR for U.S. pre-screening purposes, the handling of PNR data under the Interim Agreement, and any complaints from EU citizens or official entities related to DHS’s handling of PNR data. Exhibit A to plaintiff’s motion for partial summary judgment at 2 (hereinafter “Interim Agreement Request”). Pursuant to DHS regulations, specifically 6 C.F.R. § 5.5(d)(1)(ii), plaintiff sought expedited processing of its request on the ground that it pertained to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity,” made by “a person primarily engaged in disseminating information.” Interim Agreement Request at 2.

In support of its assertion that there existed an “urgency to inform the public” about the subject matter of its request, plaintiff noted that the Interim Agreement “expires on July 31, 2007, and will need to be renegotiated prior to that date.” *Id.* at 2. Plaintiff also cited two news articles reporting on the “arduous” nature of the negotiations between the United States and the EU. *Id.* In addition, plaintiff attached the first page of a printout of a Google News search for “privacy and ‘passenger data,’” which returned “about 621 results from news outlets throughout the world.” *Id.* at 3. Finally, plaintiff referenced a September 30, 2006 DHS press release, in which Secretary Chertoff announced that he had initialed a draft formal agreement regarding the

---

<sup>9</sup>Interim Agreement at Art. 6, 72 Fed. Reg. at 349; see also Reply by the Council Presidency and the Commission to the letter from the USA’s Department of Homeland Security available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/adequacy/pnr/2006\\_10\\_letter\\_council\\_reply\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_letter_council_reply_en.pdf).

continued sharing of PNR data. Id.

Plaintiff did not independently address why it was “primarily engaged in disseminating information,” but simply referred to its statements in support of its request for news media fee status. Id. In support of this latter request, plaintiff mentioned that “[o]ne of EFF’s primary objectives is ‘to educate the press, policymakers and the general public about online civil liberties.’” Id. (quoting a report on [www.guidestar.org](http://www.guidestar.org)). Plaintiff claimed that “[t]o accomplish this goal, EFF routinely and systematically disseminates information in several ways.” Id. Plaintiff then cited its web site, online newsletter, blog, research papers, books, and interviews with its staff as reasons supporting EFF’s entitlement to news media fee status. Id. at 3-4.

By letter dated November 1, 2006, DHS acknowledged receipt of plaintiff’s FOIA request and denied its request for expedited processing. Exhibit B to plaintiff’s motion for partial summary judgment at 1. This denial was based on DHS’s determination that EFF is “not primarily engaged in the disseminating of information to the public,” and that EFF’s October 20, 2006 request had not “detailed with specificity why [EFF] feel[s] there is an urgency to inform the public about” the subject matter of its request. Id. The letter continued, stating that the “urgency would need to exceed the public’s right to know about government activity generally,” and concluded by explaining to plaintiff that it “did not offer any supporting evidence of public interest that is any greater than the public’s general interest in the transfer and use of passenger name data.” Id. at 2-3.

On November 21, 2006, plaintiff appealed the denial of its request for expedited

processing, and the initial denial, later reversed, of its request for news media fee status.<sup>10</sup>

Exhibit C to plaintiff's motion for partial summary judgment at 1. In support of its appeal on the issue of whether it is "primarily engaged in disseminating information," plaintiff simply incorporated its appeal relating to its news media fee status, in which plaintiff cited the content of its most recent newsletter and its news blog. Id. In support of its appeal on the "urgency" issue, plaintiff cited a November 17, 2006 speech by Secretary Chertoff to the Federalist Society in which he referenced the negotiation of the Interim Agreement, and a Reuters article describing the speech. Id. at 2.<sup>11</sup>

## **2. Plaintiff's ATS Requests**

Plaintiff submitted two FOIA requests to DHS concerning the Automated Targeting System ("ATS"), a database tool maintained CBP to aid its mission of protecting the borders. DHS has detailed the specifics of this program, and addressed potential privacy concerns, in a System of Record Notice ("SORN") published in the Federal Register, 71 Fed. Reg. 64,543 (Nov. 2, 2006), and in a Privacy Impact Assessment dated November 22, 2006. Privacy Impact Assessment for the Automated Targeting System (attached as Exhibit 3). The SORN describes ATS as an "enforcement screening module associated with the Treasury Enforcement Communications System [(“TECS”)].” 71 Fed. Reg. at 64,543. TECS is “an overarching law enforcement information collection, and sharing environment,” which is “comprised of several modules designed to collect, maintain, and screen data, conducting targeting, and share

---

<sup>10</sup>On December 15, 2006, DHS granted plaintiff news media fee status. Accordingly, the parties are discussing a stipulation to dismiss plaintiff's claim pertaining to this fee issue.

<sup>11</sup>The text of Secretary Chertoff's speech referenced in plaintiff's November 21, 2006 letter is attached as Exhibit D to plaintiff's motion for partial summary judgment.

information.” Id. Previously, the information about the ATS was covered by the TECS SORN. Id.

ATS is not a new system and the notice DHS issued on November 2, 2006, “does not identify or create any collection of information, rather DHS is providing additional notice and transparency of the functionality of these systems.” Id. ATS is an analytical tool within TECS that uses “existing information in a number of sources” to screen and establish risk assessments for “inbound and outbound cargo, travelers and conveyances.” Id. The Privacy Impact Assessment makes clear that the ATS’s “sources of information” do not come “directly from individuals.” See Privacy Impact Assessment at 7. Rather, personally identifiable information is “collected from government data sources and private entities in accordance with U.S. legal requirements or other applicable arrangements,” and is used “to ensure that people and cargo entering or exiting the United States comply will all applicable U.S. laws.” Id.

**a. November 7, 2006, Request**

On November 7, 2006, plaintiff submitted to DHS’s Departmental Disclosure and Privacy Office a request for expedited processing for material concerning the ATS. Exhibit E to plaintiff’s motion for summary judgment (hereinafter “First ATS Request”). In support of its request for expedition, plaintiff asserted that the request “pertains to a matter about which there is an ‘urgency to inform the public about an actual or alleged federal government activity,’ and the request is made by ‘a person primarily engaged in disseminating information.’” Id. at 2 (citing 6 C.F.R. § 5.5(d)(1)(ii)). Plaintiff relied on a search of Google News that revealed 58 results for articles that cited the phrase “automated targeting system” to argue that “there is substantial public interest in the Department’s use of the ATS.” Id. at 2. Plaintiff did not

account for the fact that some of those 58 results were duplicates. Compare, e.g., id. at 6 (the Wilmington Morning Star, the Helena Independent Record and the Wyoming News all state that “[t]he notice provides details of the Automated Targeting System, which, it said, processes and stores information on travelers”) with id. at 10 (the Associated Press story that is reproduced in USA Today that states that “[t]he notice provides details of the Automated Targeting System, which, it said, processes and stores information on travelers”). Plaintiff did not explain whether the news sources that were identified by the Google News search were located in the United States, whether they were reporting to an American audience, or whether these articles reached a wide audience.

After going through the alleged “substantial public interest” about the ATS, plaintiff claimed that “there is an ‘urgency to inform the public’ about the potential privacy implications of the ATS because the Department has solicited public comments and that ‘[t]he new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination.’” Id. at 3 (quoting 71 Fed. Reg. 64,543). Plaintiff articulated that the “purpose of this request is to obtain information directly relevant to DHS’s Privacy Act notice” and that there is allegedly an urgency to inform the public “in order to facilitate full and informed public comment on the issue prior to the December 4 deadline the Department has imposed.” Id.

In its section on expedited processing, plaintiff did not explain how it is “primarily engaged in disseminating information,” but rather just referred to the section below that discussed its request for news media fee status. Id. In that latter section, plaintiff mentioned that “[o]ne of EFF’s primary objectives is ‘to educate the press, policymakers and the general public

about online civil liberties.” Id. (quoting a report on [www.guidestar.org](http://www.guidestar.org)). Plaintiff claimed that “[t]o accomplish this goal, EFF routinely and systematically disseminates information in several ways.” Id. Plaintiff then cited its web site, online newsletter, blog, research papers, books, and interviews with its staff as being illustrative of how it should get news media fee status. Id. at 4.

**b. December 6, 2006, Request**

On December 6, 2006, plaintiff submitted a second request concerning the ATS. Exhibit F to plaintiff’s motion for partial summary judgment (hereinafter “Second ATS Request”). This more extensive request included eight separate line items, with the final paragraph including ten subparagraphs. Id. at 1-3. An example of the breadth of its requests is that EFF seeks “all records that discuss or identify the number of individuals who have been arrested as a result of screening by the ATS, and the offenses for which they were charged.” Id. at 2.

Plaintiff’s arguments in this letter for why it feels entitled to expedited processing were similar to what it mentioned in its November 7, 2006 letter. Again, plaintiff relied on DHS’s standard for determining expedited processing. Again, plaintiff focused on why there is an alleged substantial public interest before discussing the reasons it thinks there is an urgency to inform the American public; plaintiff referenced the search results in Google News and cited articles from the Washington Post and the Associated Press. Id. at 3 (claiming that “almost 900 articles have been published that discuss the system and the privacy issues it raises”).

Plaintiff also put forth similar arguments as it put forth in its November 7, 2006 letter for why there is allegedly an “urgency to inform the public.” Plaintiff expressed the desire to “facilitate full and informed public comment and debate on [the Privacy Act notice] prior to the

new December 29 deadline the Department has imposed . . . .” Id. at 3-4.<sup>12</sup> However, in addition to the public comment deadline, plaintiff argued that because two senators and a congressman commented on the program, one of the purposes of the request was to get information about the program “prior to the Congressional consideration of the system when the new Congress convenes in January.” Id. at 3.

With regard to the question whether plaintiff is “primarily engaged in disseminating information,” plaintiff put forth the same argument that it put forth in its November 7, 2006 request, relying completely on its separate representations on the question whether plaintiff is entitled to news media fee status. Compare First ATS Request at 2-3 with Second ATS Request at 4-5. Plaintiff added that DHS had previously found that EFF qualified as news media for fee purposes. See Second ATS Request at 4.

**c. DHS’s Response to Plaintiff’s ATS Requests**

On November 14, 2007, DHS acknowledged plaintiff’s November 7, 2006, request. See letter from DHS to EFF, dated November 14, 2006 (“DHS Initial Response”) (attached as Exhibit 4). After plaintiff submitted its second request on December 6, 2006, DHS responded by informing plaintiff that it “aggregated [the requests] to simplify processing” and denoted “a consolidated list of records requested.” See letter from DHS to EFF, dated December 14, 2006 (“DHS Consolidated Response”) (attached as Exhibit G to plaintiff’s motion for partial summary judgment). In this December 14, 2006, letter, the DHS Disclosure and Privacy Office denied plaintiff’s “request for expedited treatment.” Id. at 3. Although DHS determined that plaintiff

---

<sup>12</sup>Subsequent to plaintiff’s First ATS Request, the deadline for public comments relating to the Privacy Act notice was postponed from December 4, 2006 to December 29, 2006. See 71 Fed. Reg. 71,182, 71,182 (Dec. 8, 2006).

would be considered news media for fee purposes, the agency determined that “EFF [is] not primarily engaged in disseminating information to the public.” Id. The agency also determined that EFF is not entitled to expedited processing because it did not “detail[] with specificity why [it feels] there is an urgency to inform the public about this topic.” Id. Specifically, DHS mentioned that the “urgency would need to exceed the public right to know about government activity generally” and that EFF “did not offer any supporting evidence of public interest that is any greater than the public’s general interest in personal privacy protection.” Id. In this letter, DHS also informed EFF of its right to appeal any fee waiver or expedited treatment determination “within 60 days of receipt of this letter.” Id.<sup>13</sup>

### ARGUMENT

Plaintiff’s requests for expedited processing fail to satisfy the statutory and regulatory standards, and therefore summary judgment affirming the agency’s denial of these requests is appropriate. As an initial matter, plaintiff did not exhaust its administrative remedies for the ATS Requests and therefore this Court lacks subject-matter jurisdiction over plaintiff’s claim for expedited processing of these requests. See Oglesby v. Dep’t of Army, 920 F.2d 57, 61-62 (D.C. Cir. 1990). Furthermore, with respect to the Interim Agreement Request and the ATS Requests, plaintiff is not “primarily engaged in disseminating information,” nor has plaintiff demonstrated an “urgency to inform” the American public about the subject matter of its requests. 5 U.S.C. § 552(a)(6)(E)(ii); 6 C.F.R. § 5.5(d)(1)(ii). Accordingly, defendant is entitled to partial summary judgment on plaintiff’s claims for expedited processing and plaintiff’s motion for partial

---

<sup>13</sup>On January 23, 2007, DHS sent a letter to plaintiff proposing ways to limit the scope of the ATS request. Plaintiff responded on February 15, 2007 with an agreement to limit parts of the request.

summary judgment should be denied.

**A. EFF Never Exhausted its Administrative Remedies for its ATS Requests**

“It is well settled that full and timely exhaustion of administrative remedies is a prerequisite to judicial review under FOIA.” Judicial Watch, Inc. v. United States Naval Observatory, 160 F.Supp.2d 111, 112 (D.D.C. 2001); accord Spannaus v. U.S. Dep’t of Justice, 824 F.2d 52, 58 (D.C. Cir. 1987) (“[i]t goes without saying that exhaustion of remedies is required in FOIA cases”) (internal citation omitted); Oglesby, 920 F.2d at 61-62 (“[c]ourts have consistently confirmed that the FOIA requires exhaustion of [the agency’s] appeal process before an individual may seek relief in the courts”); 6 C.F.R. § 5.9 (DHS regulation implementing FOIA’s exhaustion requirement administratively). “Where plaintiff has failed to exhaust its administrative remedies prior to filing with the court, the case is subject to dismissal for lack of subject matter jurisdiction.” Judicial Watch v. United States Naval Observatory, 160 F.Supp.2d at 112; accord Judicial Watch v. Federal Bureau of Investigation, 190 F.Supp.2d 29, 33 (D.D.C. 2002).<sup>14</sup>

E-FOIA specifically requires agencies to promulgate regulations ensuring that administrative appeals of the denial of a request for expedited processing will be considered expeditiously. 5 U.S.C. § 552(a)(6)(E)(ii)(II). DHS has enacted regulations specifically governing appeals of expedition denials. Under the regulations, denials of requests for expedited

---

<sup>14</sup>There is one exception to this rule. A requestor may “constructively” exhaust administrative remedies if an agency fails timely to respond to a FOIA requestor and the requestor sues before the agency cures its failure to respond. See, e.g., Oglesby, 920 F.2d at 63-66. Because DHS responded to plaintiff’s request for expedited processing within the statutory time-frame for the Second ATS Request (and before plaintiff filed suit on the First ATS Request), there is no question of constructive exhaustion on the expedition issue in this case.

processing are “adverse determinations” subject to the Department’s administrative appeal process, 6 C.F.R. § 5.6(c), and administrative appeals “shall be acted on expeditiously.” 6 C.F.R. § 5.5(d)(4). The regulations specifically inform requestors that “[i]f you wish to seek review by a court of *any* adverse determination, you must first appeal it under this section.” 6 C.F.R. § 5.9(c) (emphasis added).

Defendant respectfully asks this Court to reexamine its position that a requester is not required to appeal a denial of expedited processing before seeking judicial review. See ACLU v. DOJ, 321 F.Supp.2d 24, 28 (D.D.C. 2004). According to this Court, because FOIA “specifically authorizes judicial review for challenges to ‘[a]gency action *to deny or affirm denial of* a request for expedited processing,’ id. (emphasis in original) (quoting 5 U.S.C. § 552(a)(6)(E)(iii), “judicial review is appropriate at either of two moments: when the agency has denied a request for expedited processing, or when the agency has, upon administrative appeal, affirmed the denial of such a request.” Id. (quoting Al-Fayed v. CIA, Case No. 00-2092, 2000 WL 34342564, at \*2 (D.D.C. Sept. 20, 2000), aff’d on other grounds, 254 F.3d 300, 311 (D.C. Cir. 2001).

Defendant contends that FOIA contemplates judicial review only after a requester has appealed an agency’s adverse determination of its request for expedited processing. The relevant provision states that “[a]gency action *to deny or affirm denial of* a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review.” 5 U.S.C. § 552(a)(6)(E)(iii). This provision can be read as contemplating judicial review in three circumstances: (i) where the agency denies expedited processing, the requestor appeals, and the agency does not timely

respond to the appeal (“agency action to deny”); (ii) where the agency denies expedited processing, the requestor appeals, and the agency affirms the denial on appeal (“agency action to . . . affirm denial”); and (iii) where the agency does not timely respond to a request for expedited processing and plaintiff files suit before receiving a response (“failure by an agency to respond in a timely manner”).<sup>15</sup> This is the only reading consistent with § 552(a)(6)(E)(ii)(II), which commands agencies to create an administrative appeals process for resolving expedition appeals “expeditious[ly],” the DHS regulations implementing § 552(a)(6)(E)(ii)(II), and the long line of cases requiring exhaustion as a condition precedent to invoking FOIA’s judicial review provision.

It is hard to fathom that Congress would not have been more explicit if it meant to allow requestors to bypass the administrative process and go straight to court to challenge expedition denials. Congress, in 1996, was legislating against a long and consistent history of courts requiring exhaustion under FOIA. *See, e.g., Stebbins v. Nationwide Mut. Ins. Co.*, 757 F.2d 364, 366 (D.C. Cir. 1985); *Crooker v. United States Secret Serv.*, 577 F. Supp. 1218, 1219 (D.D.C. 1983). Congress would not likely have departed from this highly developed case law without some acknowledgment it was doing so. *Cf. White v. Mercury Marine*, 129 F.3d 1428, 1434 (11th Cir. 1997) (“Congress is assumed to act with the knowledge of existing case law and interpretations when it passes new legislation.”). In addition, the case law makes clear that

---

<sup>15</sup>These three scenarios are consistent with the D.C. Circuit's description of exhaustion in *Oglesby*. *See* 920 F.2d at 65-66 (“Where, as discussed below, appellant has not constructively exhausted his claims, he must appeal to the agencies within 60 days from the date of the district court’s order on remand from this court. Following his administrative appeals, or if the agencies do not respond within twenty days of the appeal, the appellant will be deemed to have fully exhausted his administrative remedies and may bring suit.”) (footnote omitted).

exhaustion is not limited to agency withholding decisions, but also applies to an agency's refusal to waive fees. See Oglesby, 920 F.2d at 66; Judicial Watch, Inc. v. Federal Bureau of Investigation, 190 F.Supp.2d at 33; see also 6 C.F.R. 5.6(c) (determination of any disputed fee matter is an "adverse determination" subject to DHS administrative appeal process). Courts require exhaustion in the fee waiver context even though the statute says only: "In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo," 5 U.S.C. § 552(a)(4)(A)(vii). Furthermore, unlike the expedited processing provisions, the fee waiver provision does not mention an agency appeals process.

Congress explicitly connected the judicial review process for a denial of expedited processing with the process for a denial of a fee waiver. The expedited processing section in the FOIA statute expressly "directs that [Section 552(a)(4)] shall govern review of denials of expedition with only one exception." Al-Fayed, 254 F.3d at 305 (citing 5 U.S.C. § 552(a)(6)(E)(iii)).<sup>16</sup> As explained above, the D.C. Circuit has long held that FOIA plaintiffs must exhaust administrative remedies before filing suit under § 552(a)(4), the provision that governs fee waivers. See, e.g., Oglesby, 920 F.2d at 61-62, 66. Indeed, the Court of Appeals requires exhaustion in part because "[t]he statutory scheme in the FOIA specifically provides for an administrative appeal process following an agency's denial of a FOIA request." Id. at 61 (citing 5 U.S.C. § 552(a)(6)(A)(i), (ii)). So, too, the statute specifically provides for an administrative appeals process following an agency's denial of expedition. See 5 U.S.C. § 552(a)(6)(E)(ii) (requiring agencies to enact regulations ensuring (i) that determinations of

---

<sup>16</sup>The exception is that judicial review of an expedition decision is on the agency record. See 5 U.S.C. § 552(a)(6)(E)(iii); Al-Fayed, 254 F.3d at 305.

whether to provide expedited processing are made and notice provided within ten days of the date of the request and (ii) requiring “expeditious consideration” of administrative appeals of such determinations).

Requiring appeals of expedition decisions when an agency responds before suit is filed also serves the important policies underlying FOIA’s exhaustion requirement. See Hidalgo v. FBI, 344 F.3d 1256, 1258-59 (D.C.Cir. 2003) (failure to exhaust precludes review if the “‘purposes of exhaustion’ and the ‘particular administrative scheme’ support such a bar”) (internal citation omitted). For example, requiring exhaustion would: (i) “prevent[] premature interference with agency processes,” (ii) “compil[e] a record which is adequate for judicial review,” and (iii) preserve the “agency’s power to correct or rethink initial misjudgments or errors.” Id. at 1259-60 (internal citations and quotations omitted); see also Dettmann v. DOJ, 802 F.2d 1472, 1476-77 & n.8 (D.C. Cir. 1986) (discussing other policies underlying exhaustion requirement).

Plaintiff should not be rewarded for its efforts to bypass the administrative process. Plaintiff would not have been able to bypass the process for a denial of a fee waiver and it should not be allowed to bypass the process for a denial of expedited processing. Accordingly, plaintiff’s claims for expedition with respect to the ATS Requests should be dismissed for failure to exhaust. Separately, even if exhaustion is not required, plaintiff failed to demonstrate that it meets the statutory and regulatory standards for expedition for both the Interim Agreement and the ATS Requests.

**B. EFF Is Not Primarily Engaged in Disseminating Information.**

Plaintiff is not “primarily engaged in disseminating information,” and therefore not

entitled to expedited processing. 5 U.S.C. § 552(a)(6)(E)(ii); 6 C.F.R. § 5.5(d)(1)(ii). The E-FOIA House Report expressly states that “[t]he specified categories for compelling need are intended to be narrowly applied.” H.R. Rep. No. 104-795, at 26 (1996); see also Al-Fayed, 254 F.3d at 310. Since all FOIA requesters are likely to be “engaged in disseminating information” to some extent, the word “primarily” should be interpreted in a way that constrains grants of expedited processing to ensure that the exception to ordinary processing is “narrowly applied.”

This point was emphasized by the House Report:

A person “primarily engaged” in the dissemination of information should not include individuals who are engaged only incidentally in the dissemination of information. The standard of “primarily engaged” requires that information dissemination be the *main* activity of the requestor, although it need not be their sole occupation. A requestor who only incidentally engages in information dissemination, besides other activities, would not satisfy this requirement.

H.R. Rep. No. 104-795, at 26 (emphasis added). DHS regulations reflect this legislative intent by requiring those requesting expedited processing to “establish that he or she is a person whose *main* professional activity or occupation is information dissemination, though it need not be his or her sole occupation.” 6 C.F.R. § 5.5(d)(3) (emphasis added).

Heedless of this clear requirement, plaintiff requested expedited processing of all three of its requests without proffering evidence that its *primary* objective is to disseminate information to the public. See Al-Fayed, 254 F.3d at 305 n.4 (burden is on the requestor to demonstrate entitlement to expedited processing) (quoting 5 U.S.C. § 552(a)(6)(E)(i)(I); H.R. Rep. No. 104-795, at 25). Indeed, in all of its requests for expedition, plaintiff relied on evidence proffered in support of its request for news media fee status to prove that it is “primarily engaged in disseminating information.” See Interim Agreement Request at 3 (“as I explain below in support of our request for ‘news media’ treatment, EFF is ‘primarily engaged in disseminating

information”); First ATS Request at 2 (same); Second ATS Request at 4 (same). By conflating the standard for determining when a requester is a “representative of the news media” with the standard for determining when a requester is “primarily engaged in disseminating information,” plaintiff has failed to appreciate that an organization may be a “representative of the news media” without being “primarily engaged in disseminating information.” Indeed, this is precisely the case with respect to plaintiff.

The news media standard and the primarily engaged standard relate to different provisions with different underlying purposes. As discussed above, the “primarily engaged in disseminating information” standard is to be “narrowly applied” in order to avoid unfairly disadvantaging requestors who do not obtain expedited processing. H.R. Rep. No. 104-795, at 26. The drafters of the E-FOIA amendments recognized that “[g]iven the finite resources generally available for fulfilling FOIA requests, unduly generous use of the expedited processing procedure would unfairly disadvantage other requestors who do not qualify for its treatment.” Id. Indeed, as the D.C. Circuit has recognized, “an unduly generous approach would also disadvantage those requestors who do qualify for expedition, because prioritizing all requests would effectively prioritize none.” Al-Fayed, 254 F.3d at 310.<sup>17</sup>

By contrast, agencies are instructed to take a generous approach to grants of news media fee status. The “representative of the news media” standard is to be “broadly interpreted”

---

<sup>17</sup>The D.C. Circuit has also recognized that FOIA requestors should not be able to avoid the general rule that FOIA requests are processed in the order they are received simply by filing a lawsuit. Open Am. v. Watergate Special Prosecution Force, 547 F.2d 605, 615 (D.C. Cir. 1976) (“[i]f everyone could go to court when his request had not been processed within thirty days, and by filing a court action automatically go to the head of the line at the agency, we would soon have a listing based on priority in filing lawsuits, i. e., first in court, first out of the agency.”).

consistent with the purpose of the fee waiver provision of encouraging the dissemination of information in government files. National Security Archive v. Department of Defense, 880 F.2d 1381, 1386 (D.C. Cir. 1989), cert. denied, 494 U.S. 1029 (1990); Electronic Privacy Information Center v. Department of Defense, 241 F. Supp. 2d 5, 10 (D.D.C. 2003). Accordingly, “any person or organization which regularly publishes or disseminates information to the public . . . should qualify for [fee] waivers as a representative of the news media.” National Security Archive, 880 F.2d at 1386 (internal quotations and citations omitted). Thus, because agencies are directed to adopt different approaches to these determinations, a requester who obtains news media status because of an agency’s generous approach to fee issues is not necessarily entitled to status as one “primarily engaged in disseminating information.”

DHS regulations reflect this clear difference. The regulations define a “representative of the news media” as “any person actively gathering news for an entity that is organized and operated to publish news to the public.” See 6 C.F.R. § 5.11(b)(6). However, the regulation clearly contemplates that disseminating information to the public need not be the requestor’s primary objective, so long as it is one of its activities. See id. (“a request for records supporting the *news-dissemination function* of the requestor shall not be considered to be for a commercial use”) (emphasis added). By contrast, DHS regulations require a requester seeking expedited processing who is not a “*full-time* member of the news media” to “establish that he or she is a person whose *main* professional activity or occupation is information dissemination.” 6 C.F.R. § 5.5(d)(3) (emphasis added). The grant of news media status does not establish that a person is a “full-time” member of the news media, or that the person’s “main professional activity” is

news dissemination.<sup>18</sup>

To be found to be primarily engaged in disseminating information, plaintiff would have had to show that informing the public is its main activity as opposed to being one of a litany of activities. See ACLU-NC v. Dep't of Justice, Case No. C 04-4447, 2005 WL 588354 at \*14 (N.D. Cal. March 11, 2005) (“the court agrees with defendants that while dissemination of information may be *a* main activity, there is no showing that it is *the* main activity”) (emphasis in original). An organization can have only one “primary” activity. See id. (“ACLU-NC argued that ‘primary’ could refer to more than one – that two or more activities could be ‘primary.’ As defendants have pointed out, however this interpretation is not supported by the either the DOJ regulations or the legislative history”). To be entitled to expedited processing of its requests, plaintiff has the burden of demonstrating that its “primary” activity is disseminating information. While some disseminating activities may be sufficient for news media status, it is not sufficient for expedited processing.<sup>19</sup>

---

<sup>18</sup>Plaintiff’s citation to different agencies’ regulations has little probative value since those regulations are not at issue, and because this court must interpret the statute *de novo*. See Al-Fayed, 254 F.3d at 307 (“district courts may not defer to any individual agency’s effort to elaborate upon [the definition of compelling need].”).

<sup>19</sup>This issue was not squarely presented in ACLU v. Dep't of Justice, 321 F.Supp.2d 24 (D.D.C. 2004), and therefore plaintiff’s reliance on this case is misplaced. In ACLU, the issue of whether the Electronic Privacy Information Center (“EPIC”) was “primarily engaged in disseminating information” was not the central issue before the Court. In fact, this Court stated that “[t]he government’s position regarding the issue is left unclear, but it seems to have abandoned this ground for refusal to expedite the request.” Id. at 29 n.5. Nevertheless, the Court stated that “if the government did not intend to concede EPIC’s status, the Court concludes that EPIC is indeed ‘primarily engaged in disseminating information’ for the purposes of expediting the request.” Id. In reaching this conclusion, this Court gave a synopsis of EPIC’s activities by citing a case that granted EPIC news media fee status. Id. (citing Electronic Privacy Information Center v. Dep't of Defense, 241 F.Supp. 2d 5, 10 (D.D.C. 2003)). By relying on that case as a synopsis of EPIC’s activities, this Court did not conclude that there is a connection between

While plaintiff does engage in some news dissemination activities, it is primarily in the business of litigating. See ACLU-NC v. Dep't of Justice, Case No. C 04-4447, 2005 WL 588354 at \*14 (N.D. Cal. March 11, 2005) (finding that the ACLU-NC is not entitled to expedited processing of FOIA requests at issue). This fact is trumpeted on plaintiff's website, which states that "EFF fights for freedom *primarily* in the courts even when that means taking on the U.S. government or large corporations." About EFF, *available at* [www.eff.org/about](http://www.eff.org/about) (attached as Exhibit 5). Consistent with this representation, in its requests to DHS, plaintiff did not state that its primary objective is to disseminate information, but that "[o]ne of EFF's *primary objectives* is 'to educate the press, policymakers and the general public about online civil liberties.'" Interim Agreement Request at 3 (emphasis added); First ATS Request at 2 (same); Second ATS Request at 4 (same). This quotation is plucked from a more complete description of plaintiff presented in a Guidestar Basic Report cited in all three of plaintiff's requests, which provides, in full, as follows:

The Electronic Frontier Foundation (EFF) works on issues of free expression, freedom of press, privacy, anonymity, security, and fair use, among many others, as they relate to computing and the Internet. EFF's objectives are to ensure that our fundamental rights are at least as well-secured online as they are offline; to educate the press, policymakers and the general public about online civil liberties; and to act as a defender of those liberties when they are attacked. *Among our various activities*, EFF opposes misguided legislation, defends individuals' rights in court, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, supports the development of new communication technologies, engages the press daily, and publishes a comprehensive archive of online civil liberties information on our website: <http://www.eff.org>. We pride ourselves on being the first to see potentially threatening issues on the horizon and to take pre-emptive action to protect civil

---

being news media for fee purposes and being primarily engaged in disseminating information for purposes of expedition. If the Court did indeed make such a connection, defendant respectfully requests that it reexamine its previous position in light of the arguments put forth in these papers.

liberties on the Internet.

Guidestar Basic Report, Electronic Frontier Foundation at 2, available at <http://www.guidestar.org/pqShowGsReport.do?npoID=5616245> (attached as Exhibit 6) (emphasis added). Further, under the “Additional Comments from the Organization” section of this report, plaintiff’s only additional comment was that:

Three of the most important legal cases of the last decade for electronic communications have been EFF cases: Steven Jackson Games v. U.S. Secret Service (email privacy), Bernstein v. U.S. Department of Justice (export controls on encryption, which defined computer code, for the first time, as a form of expression that is protected by the First Amendment), and Universal Studios, v. Reimerdes (copyright fair use).

Id. at 3. As this report and EFF’s website make clear, dissemination of information is not plaintiff’s primary activity, but is merely incidental to its primary activity, defending online civil liberties in court. Accordingly, plaintiff is not entitled to expedited processing.

**C. There Was No “Urgency to Inform” the Public About the Federal Government Activity at Issue in Plaintiff’s FOIA Requests**

Even if plaintiff is primarily engaged in disseminating information, plaintiff would still not be entitled to expedited processing because it has failed to demonstrate an urgency to inform the American public regarding either the Interim Agreement or the Automated Targeting System.

In keeping with the congressional mandate that the categories for compelling need are to be narrowly applied, Congress described the “urgency to inform” standard as follows:

The standard of “urgency to inform” requires that the information requested should pertain to a matter of a current exigency to the American public and that a reasonable person might conclude that the consequences of delaying a response to a FOIA request would compromise a significant recognized interest. The public’s right to know, although a significant and important value, would not by itself be sufficient to satisfy this standard.

H.R. Rep. No. 104-795, at 26; see also Al-Fayed, 254 F.3d at 310. Thus, courts consider three

factors in determining whether a requestor has demonstrated an “urgency to inform”: (1) whether the request concerns a matter of current exigency to the American public; (2) whether the consequences of delaying a response would compromise a significant recognized interest; and (3) whether the request concerns federal government activity. Plaintiff’s requests failed to satisfy factors (1) and (2).<sup>20</sup>

Importantly, this Court’s review of whether plaintiff’s request satisfied the “urgency to inform” standard is restricted to the record as it existed before DHS when it denied plaintiff’s expedition request. 5 U.S.C. 552(a)(6)(E)(iii); Al-Fayed, 254 F.3d at 304. The burden is on the requestor to demonstrate that its expedition request was warranted. See Al-Fayed, 254 F.3d at 305 n.4 (quoting H.R. Rep. No. 104-795, at 25); see also 6 C.F.R. § 5.5(d)(3) (burden is on requestor to explain in detail the basis for requesting expedited processing). The record is comprised of plaintiff’s initial FOIA requests as well as its appeal of the denial of its request for expedited processing of the Interim Agreement Request. This record fails to prevent sufficient evidence that the subject matter of plaintiff’s requests concerned a matter of “current exigency to the American public,” or that processing plaintiff’s requests in the ordinary course would “compromise a significant recognized interest.”

**1. Plaintiff Failed to Demonstrate that there is an Urgency to Inform the American Public about the Interim Agreement**

Plaintiff’s October 20, 2006 FOIA request for information relating to the Interim Agreement does not concern a matter of “current exigency to the American public,” nor would processing the Interim Agreement Request in the ordinary course “compromise a significant

---

<sup>20</sup>Defendant does not dispute that plaintiff’s FOIA request concerns federal government activity.

recognized interest.” Al-Fayed, 254 F.3d at 310. This fact presents an independent reason to affirm defendant’s denial of plaintiff’s request for expedited processing.

Plaintiff failed to demonstrate that the agency records requested by the Interim Agreement Request concern a matter of “current exigency to the American public” chiefly for the reason succinctly stated in defendant’s November 1, 2006 letter denying plaintiff’s request for expedited processing: plaintiff “did not offer any supporting evidence of public interest [in the negotiation of the Interim Agreement] that is any greater than the public’s general interest in the transfer and use of passenger name data.” Exhibit B to plaintiff’s motion for partial summary judgment at 1.

As this statement acknowledges, the debate over whether the government should have access to PNR data contained in airline reservation systems to aid the government in its quest to prevent further terrorist attacks is simply one part of the larger debate over the appropriate balance between national security and personal privacy. In the *United States*, the particular debate over the transfer of PNR data to the government came to a head and was resolved in November 2001, when this nation’s elected representatives enacted the Aviation and Transportation Security Act, mandating that “carriers shall make passenger name record information available to the Customs Service upon request.” 49 U.S.C. § 44909(c)(3). Of course, the *American* public, acting through its elected representatives, may always revisit this resolution, but plaintiff’s Interim Agreement Request provides no evidence of any current interest of the *American* public to do so.

The evidence plaintiff does cite in its Interim Agreement Request, at most, suggests that the information sought by that request—under what terms may our government have access to

PNR data collected by carriers in connection with flights from the EU to the U.S.—is a matter of current interest to the *European* public. The Interim Agreement, and the 2004 Agreement that preceded it, were prompted by a possible conflict between the requirements of the Aviation and Transportation Security Act and *European* privacy law. Thus, the purpose of both the 2004 Agreement and the Interim Agreement is to address *European* discomfort with the obligations imposed by the Aviation and Transportation Security Act and its implementing regulations on air carriers operating flights between the EU and the U.S. Given this fact, it is not surprising that plaintiff requested “complaints received from *EU citizens or official entities* concerning DHS acquisition, maintenance and use of passenger data of *EU citizens*,” but did not request any complaints received from U.S. citizens or official entities. Interim Agreement Request at 2. Similarly, the news articles cited in the Interim Agreement Request in support of plaintiff’s request for expedited processing all address *European* interest in the negotiations. For example, the Interim Agreement Request quotes extensively from a Reuters Article that repeatedly emphasizes the concerns of *Europeans* over U.S. collection of personal data:

*EU* lawmakers raised worries that Washington was riding roughshod over data protection concerns in its quest after September 11, 2001 attacks to further a “war on terrorism” whose tactics many *Europeans* question. One *Greek* left-wing deputy accused the EU of having “totally caved in” to U.S. pressure.

Interim Agreement Request at 2 (quoting Reuters, *Europe Reach Deal on Air Passenger Data*, Oct. 6, 2006) (emphasis added). Absent from this news article is any mention of American interest in the Interim Agreement.

Likewise, the Google News printout attached to the Interim Agreement Request does not demonstrate any significant *American* interest in the negotiation and conclusion of the Interim Agreement. Google News “aggregates headlines from more than 4,500 English language news

sources worldwide,” without regard to the popularity of the news source or the nationality of its intended audience.<sup>21</sup> Plaintiff’s reliance on its Google News search to demonstrate its entitlement to expedited processing is flawed in several respects. First, the sheer number of news outlets aggregated by Google News ensures that almost any search will return a seemingly large number of results. Thus, while 621 results may seem like an impressive figure in the abstract, it pales in comparison to Google News searches related to issues that actually interest the American public. Thus, for example, a February 15, 2007 Google News search for articles containing the terms “Iran and Nuclear and ‘United States’” returned 17,457 results. See Exhibit 7. A similar search for “Surge and Iraq” returned 15,142 results. See Exhibit 8. Second, Google News collects English language news from around the world and therefore does not distinguish between stories that are of interest to the *American* public, and those that are of interest to the rest of the English speaking world. See e.g., Exhibit 9 (February 16, 2007 Google News search for “cricket and match” returns 11,547 articles). Finally, plaintiff’s search term is vague and overly broad, and its failure to attach more than the first page of its search results prevents DHS from ascertaining whether these news articles concerned the negotiation of the Interim Agreement or some other aspect of “privacy and ‘passenger data.’” See Interim Agreement Request at 6. The only major American newspaper to appear on the Google News printout attached to the Interim Agreement Request is the Washington Post, and the existence of this lone article surely does not demonstrate that “the request concerns a matter of current exigency to the *American* public.” Al-Fayed, 254 F.3d at 310 (emphasis added).

---

<sup>21</sup>About Google News, available at [http://news.google.com/intl/en\\_us/about\\_google\\_news.html](http://news.google.com/intl/en_us/about_google_news.html)

To the extent the Interim Agreement Request demonstrates any *American* media interest, it is media interest regarding the impact of the Interim Agreement negotiations on the relationship between the United States and the European Union—not media interest concerning the impact of the Interim Agreement on Americans’ privacy. Thus, the EU-U.S. relationship is the subject of both the Associated Press article and the DHS press release cited by plaintiff in its Interim Agreement Request. The Associated Press article speaks of the “arduous” nature of the negotiations that “reflected deep divisions between the United States and the European Union.” Interim Agreement Request at 2. Similarly, Secretary Chertoff’s comments upon the initialing of the draft Interim Agreement do not reflect any particularly acute American debate about the privacy impact of PNR collection, but were simply intended to “inform[] the public of developments in the negotiations with the EU.” *Id.* at 3. Likewise, Secretary Chertoff’s comments to the Federalist Society on the issue of international and transnational law, in which he mentioned “very substantial debate” over the Interim Agreement as an example of when foreign law attempts to impose limits on valid U.S. law, hardly demonstrates the exigent nature of plaintiff’s request to the American public. See Exhibit D to plaintiff’s motion for partial summary judgment.

While the United States’ relationship with its European allies is clearly a matter of great importance, plaintiff fails to demonstrate why the impact of the Interim Agreement on the EU-U.S. relationship is of any greater interest to the American public than a myriad of other issues relating to trade, the environment, foreign policy, and countless other matters that impact the EU-U.S. relationship. See e.g., End-of-Year Remarks of Daniel Fried, Assistant Secretary of State for European and Eurasian Affairs, December 12, 2006, attached as Exhibit 10. The

public's right to know about information related to the Interim Agreement, like the public's right to know about every aspect of the EU-U.S. relationship, "is a significant and important value," but it is "not by itself [] sufficient to satisfy" the requirements for expedited processing. Al-Fayed, 254 F.3d at 310 (quoting H.R.Rep No. 104-795, at 26). In short, plaintiff has failed to demonstrate that the Interim Agreement Request "concerns a matter of current exigency to the American public." Id.

Likewise, plaintiff fails to demonstrate that "the consequences of delaying a response would compromise a significant recognized interest," chiefly because the "interests" at stake are those of Europeans and not Americans. Id. As noted above, the debate over whether American law should require the transfer of PNR data to the government has been settled in various steps over the last several years: (i) when Congress enacted and the President signed the Aviation and Transportation Security Act in 2001, (ii) when the interim regulation implementing this statute was promulgated in 2002, (iii) when Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act of 2004, and (iv) when the President issued Exec. Order No. 13,388. The legal obligations imposed by these validly enacted laws, validly promulgated regulation, and validly issued Executive Order apply to anyone who crosses United States' borders, and will continue to apply to anyone who crosses United States' borders irrespective of the results of the renegotiation of the Interim Agreement. See 72 Fed. Reg. at 349. As the Interim Agreement clearly states: "This Agreement is not intended to derogate from or amend legislation of the United States of America . . . . This Agreement does not create or confer any right or benefit on any other person or entity, private or public." Id. It should come as little surprise that the Interim Agreement has generated little interest in this country. Its effect on

Americans is minimal.

Thus, this case is easily distinguishable from ACLU v. DOJ, 321 F.Supp.2d 24 (D.D.C. 2004), in which this Court held that a request for information relating to Section 215 of the Patriot Act was entitled to expedited processing because it related to the “the public’s privacy interests,” and because the information requested would contribute to “the ongoing national debate about whether Congress should renew Section 215.” Id. at 30. It is also distinguishable from Leadership Conference on Civil Rights v. Gonzales, 404 F.Supp.2d 246, 260 (D.D.C. 2005), in which this Court granted expedited processing to a request concerning the soon-to-expire Voting Rights Act. These cases involved pending *legislation* that would affect the rights and responsibilities of American citizens. The Interim Agreement does not affect the rights of American citizens, and therefore the Interim Agreement Request doesn’t concern a matter of current exigency, nor is an expedited response required to avoid compromising a significant recognized interest.

**2. Plaintiff Failed to Demonstrate that there is an Urgency to Inform the American Public about the Automated Targeting System**

Plaintiff’s original argument, made in its First ATS Request, that a December 4, 2006 deadline<sup>22</sup> created an urgent need to inform the public is no longer operative. See First ATS Request at 2 (“The purpose of this request is to obtain information directly relevant to DHS’s Privacy Act notice and the practices it describes. . . . There is clearly ‘an urgency to inform the public’ about the Department’s policies with respect to this issue in order to facilitate full and

---

<sup>22</sup>This deadline was later extended to December 29, 2006, and formed the basis of plaintiff’s Second ATS Request.

informed public comment and debate on the issue prior to the December 4 deadline the Department has imposed.”). The deadline has already passed, and thus no relief given by this Court would be able to satisfy plaintiff’s desire to have the documents before December 4, 2006. See Long v. Department of Homeland Security, 436 F.Supp.2d 38, 43 (D.D.C. 2006) (rejecting plaintiffs’ urgency argument that they needed the information to file an amicus brief to the Supreme Court because, *inter alia*, “the deadline for filing . . . has expired [and] [t]hus, it cannot be said that plaintiffs’ request concerns ‘a matter of current exigency’ or that the consequences of DHS delaying a response ‘would compromise a significant recognized interest’”) (citation omitted).

Plaintiff’s assertions of urgency are also undercut by the timing and breadth of its request. It is inconceivable that, given the breadth of the request, plaintiff would have received the documents that it desired before December 4, 2006. See First ATS Request (the request included, *inter alia*, “all records, including Privacy Act notices, that discuss or described the use of personally-identifiable information by CPB [*sic*] (or its predecessors) for purposes of ‘screening’ air and sea travelers,” dating back to the 1990’s). In any case, the request was not even made twenty business days before the December 4, 2006 deadline and thus plaintiff could not have expected to receive the documents responsive to such a broad request prior to its submission of comments to DHS’s Privacy Act notice. See 5 U.S.C. § 552(a)(6)(A)(i) (each agency shall “determine within twenty days (excepting Saturdays, Sundays and legal public holidays) after the receipts of any such request whether to comply with such request.”).

The purpose of the Second ATS Request was again to comment on the Privacy Act notice and again was not submitted in enough time for the request to conceivably have any impact on

the comments EFF submitted. See Second ATS Request at 3-4 (“The purpose of this request is to obtain information directly relevant to DHS’s Privacy Act notice and the practices it describes . . . . There is clearly ‘an urgency to inform the public’ about the Department’s policies with respect to this issue in order to facilitate full and informed public comment and debate on the issue prior to the new December 29 deadline the Department has imposed . . . .”). Again, the December 29, 2006 deadline has passed and thus no relief given by this Court would be able to satisfy plaintiff’s desire to have the documents before December 29, 2006. See Long, 436 F.Supp.2d at 43. Furthermore, the Second ATS Request was not submitted twenty working days prior to the new December 29, 2006 deadline for submission of public comments. Therefore, given the breadth of this request, EFF could not have expected to receive any documents prior to the submission deadline. See id. at 1-3 (the request includes eight paragraphs and the eighth paragraph includes ten subparagraphs).

In the Second ATS Request, plaintiff mentioned the need to lobby Congress as another rationale for there being an urgency to have its FOIA request processed out of order. See id. at 3-4 (“clearly ‘an urgency to inform the public’ about the Department’s policies with respect to this issue in order to facilitate full and informed public comment and debate on the issue prior to the new December 29 deadline the Department has imposed, and prior to the Congressional consideration of the system when the new Congress convenes in January.”). However, plaintiff did not demonstrate why lobbying Congress rises to the point of exigency for the American public. See Long, 436 F.Supp.2d at 43 (holding that participating in a debate on general policy objectives does to rise to level the urgency required for expedited processing).

Plaintiff asks this Court to hold that it is entitled to expedited processing based on the

mere possibility that Congress might conduct oversight hearings about the ATS. Plaintiff cites to a press statement by Senator Leahy and quotes from Congressman Bennie Thompson and Senator Coleman as its basis that Congress is interested in the program. See Second ATS Request at 3. However, the 535 senators and congressmen that comprise Congress deal with a great multitude of issues. The public statements of two senators and one congressman are insufficient cause to meet FOIA's narrow exception reserved to expedited processing. See H.R. Rep. No. 104-795, at 26 (1996) (“[t]he specified categories for compelling need are intended to be narrowly applied.”). Although this Court found that “sunset provisions or discussions of new legislation” can be a factor in considering whether there is an urgency to inform, it expressly stated that this justification “standing alone” may be “insufficient to demonstrate a ‘compelling need.’” ACLU v. DOJ, 321 F.Supp.2d at 31. Here, there is not even any pending legislation, sunset provision or other congressional time-frame for addressing this issue.

This case is similar to Long v. Department of Homeland Security, 436 F.Supp.2d at 43, as opposed to ACLU v. DOJ, 321 F.Supp.2d at 29, or Leadership Conference, 404 F.Supp.2d at 260. In Long, the Court rejected plaintiffs’ arguments that they were entitled to expedited processing for the need to “to inform the ongoing debate about immigration policy.” See Long, 436 F.Supp.2d at 43. The Court distinguished the case from the requests that dealt with the Patriot Act or the Voting Rights Act because in those situations “there was an ongoing public controversy associated with a *specific time frame*.” Compare id. with ACLU v. DOJ, 321 F.Supp.2d at 29 (finding that the request concerning “Section 215” of the Patriot Act “unquestionably implicates important individual liberties and privacy concerns which are of immediate public interest in view of the ongoing debate regarding the *regarding the renewal*

*and/or amendment of the Patriot Act.*”) (emphasis added) and Leadership Conference, 404 F.Supp.2d at 260 (“urgency element is met because of the *upcoming expiration* of the special provisions of the Voting Rights Act in 2007”) (emphasis added). In contrast, the plaintiffs in Long “failed to identify an imminent action indicating that the requested information ‘will not retain its value if procured through the normal FOIA channels.’” Id. (quoting Al-Fayed v. CIA, Civil Action No. 00-2092, 2000 WL 34342564, at \*5 (D.D.C. Sept. 20, 2000)). As stated above, plaintiffs have only demonstrated that three members of Congress have expressed an interest in this issue. There is no approaching deadline nor any specific time frame. Rather, plaintiff seems to want this information to create a debate about the ATS.

Besides stating the general arguments of needing to comment on the Privacy Act notice and wishing to lobby Congress, plaintiff also argues that it should get expedited processing because of the news coverage about ATS. However, news coverage is insufficient for a plaintiff to demonstrate that there is an exigency in informing the public. See Al-Fayed, 254 F.3d at 310 (subject, while “newsworthy,” was not a matter of “current exigency”). DHS does not have a regulation that allows for expedited processing for a matter of widespread media attention. See 6 C.F.R. § 5.5(d). Rather, the regulations just articulate what is in the statute; for someone to get expedited processing, the information has to affect a person’s health or there must be an exigency to inform the American public. Id. This is different from an agency such as the Department of Justice, which has a regulation that also allows for expedited processing when the matter is of “widespread and exceptional media interest.” See 28 C.F.R. § 16.5(d)(1)(iv).

Plaintiff further undermines its arguments for expedited processing because it does not even show that the American public has widespread interest in the ATS. Although pointing to

media attention is insufficient to meet the urgency to inform prong, it is still necessary for a requestor to demonstrate the American public's interest in a subject. See Electronic Privacy Information Center v. Department of Defense, 355 F.Supp.2d at 101 (“Fatal to [Electronic Privacy Information Center's] request for expedited treatment is the failure in its original FOIA to demonstrate that there is any current public interest in the specific subject of that request.”). Plaintiff's citation of obscure news sources combined with the sparse attention paid to the ATS by larger publications further reveals that there is not an urgency in the public to know about the ATS.

As explained above, the reference to a Google News search returning approximately 900 articles does not demonstrate substantial media interest in the subject. See supra, at 31; Exhibits 8-10. The Lexis-Nexis database “Major Newspapers” provides a more accurate barometer of media interest than Google News because it is restricted to newspapers with wide readership. See Source Information, Major Newspapers (attached as Exhibit 11). Unlike Google News, the Major Newspapers database does not include such sources as Officer.com, Infoshop News, Homeland Stupidity, Raw Story, or GovExec.com, which are not widely read. Compare Exhibit 11 with First ATS Request and Second ATS Request. A search conducted in the Major Newspapers database for news articles containing the term “Automated Targeting System” during the period November 1, 2006 to December 14, 2006 produces only twenty-nine results. See Lexis-Nexis search for “Automated Targeting System” (attached as Exhibit 12). Of the twenty-nine articles identified within major newspapers during those six weeks, only twenty-two of them were from the United States, and only one of these—a December 2, 2006 article in the Chicago Tribune—appeared on the front page. See Exhibit 12. Thus, despite plaintiff's bare

reference to a Google News search of global news sources, a more accurate barometer of the need to inform the public on this issue is the fact that over a six week span, the fifty largest American newspapers published only twenty-two articles mentioning the “Automated Targeting System,” only one of which appeared on the front page. This fact further demonstrates that the ATS was not at the forefront of Americans’ consciences and therefore plaintiff is not entitled to the expedited processing of its ATS Requests. See Electronic Privacy Information Center v. Department of Defense, 355 F.Supp.2d at 101.<sup>23</sup>

Lastly, plaintiff is also not entitled to expedited processing because no significant injury would result if plaintiff followed the regular procedures and waited its turn to have its FOIA request processed. EFF has no specialized interest in informing Congress. Even if a few statements made by a few congressmen discussing potential Congressional oversight and the citation of a few news articles were sufficient to show that there is an exigency to inform the public, plaintiff has not demonstrated that it has met the second prong of Al-Fayed – that “the consequences of delaying a response would compromise a significant recognized interest.” Al-Fayed, 254 F.3d at 310. Plaintiff’s primary argument here is that the public has a right to know about this program beyond what is already publicly available. However, “[t]he public's right to know, although a significant and important value, would not by itself be sufficient to satisfy” the “urgency to inform” standard. H.R. Rep. No. 104-795, at 26; Al-Fayed, 254 F.3d at 310. See also 6 C.F.R. § 5.5(d)(3) (a requestor under § 5.5(d)(1)(ii) “must establish a particular urgency to

---

<sup>23</sup>Plaintiff’s reference to a DHS policy advisor’s comment that “several media outlets were reporting” on the ATS is not part of the record and, therefore, should not be considered by the Court. See 5 U.S.C. § 552(a)(6)(E)(iii); plaintiff’s motion for partial summary judgment at 22.

inform the public about the government activity involved in the request, beyond the public's right to know about government activity generally.”). All FOIA requestors presumably have a particular interest in the information that they requested and many probably want to lobby Congress.

Plaintiff is still able to lobby Congress with the great wealth of publicly available information. See 71 Fed. Reg. 64,543 (ATS SORN); Privacy Impact Assessment (Exhibit 4). Furthermore, there is no pending legislation so plaintiff can continue to lobby Congress during the time it would typically take DHS to process plaintiff's FOIA request. Finally, Congress has the ability to conduct its own oversight and no harm would result if plaintiff does not get some of the requested information in an expedited fashion. The only significant interest that has the potential of being harmed is the delay to all other requestors as plaintiff tries to get its requests processed out of order. There is nothing in the record to suggest that allowing DHS to respond to plaintiff's request in the normal course of business will harm the American public.

Plaintiff has not met its burden in demonstrating that it needs this information in an expedited fashion and cannot wait until the normal time-frame for processing FOIA requests. Plaintiff has not shown that it is exigent for the American public to have more information about ATS nor has plaintiff shown the potential harm to a significant interest that is beyond that of other advocacy groups interested in lobbying Congress. Thus, plaintiff has failed to meet its burden and demonstrate that it has an “urgency to inform” the public about ATS just as its failed to show that it is “primarily engaged in disseminating information.”

**CONCLUSION**

For all of the foregoing reasons, defendant respectfully requests that the Court grant its motion for partial summary judgment on plaintiff's claims for expedited processing and deny plaintiff's motion for partial summary judgment.

Dated: February 22, 2007

PETER D. KEISLER  
Assistant Attorney General

JEFFREY A. TAYLOR  
United States Attorney

ELIZABETH J. SHAPIRO  
(D.C. Bar 418925)  
Assistant Branch Director  
U.S. Department of Justice  
Civil Division, Federal Programs Branch

/s/ John R. Coleman  
JOHN R. COLEMAN  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
Mailing Address  
P.O. Box 883  
Washington, D.C., 20044  
Delivery Address  
20 Massachusetts Avenue, NW, Room 6118  
Washington, D.C. 20530  
Telephone: (202) 514-4505  
Facsimile: (202) 616-8187  
john.coleman3

/s/ Adam D Kirschner  
ADAM D. KIRSCHNER  
Trial Attorneys  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
Mailing Address  
P.O. Box 883

Washington, D.C., 20044

Delivery Address

20 Massachusetts Avenue, NW, Room 7126

Washington, D.C. 20530

Telephone: (202) 353-9265

Fax: (202) 616-8470

adam.kirschner@usdoj.gov

Counsel for Defendant

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA**

<b>ELECTRONIC FRONTIER FOUNDATION</b>	)	
	)	
Plaintiff,	)	<b>Consolidated Cases</b>
	)	
v.	)	Civil Action No. 06-1988 (ESH)
	)	
<b>DEPARTMENT OF HOMELAND SECURITY</b>	)	Civil Action No. 06-2154 (RBW)
	)	
Defendant.	)	
	)	

---

**STATEMENT OF MATERIAL FACTS IN SUPPORT OF DEFENDANT'S  
MOTION FOR PARTIAL SUMMARY JUDGMENT AND IN RESPONSE TO  
PLAINTIFF'S STATEMENT OF MATERIAL FACTS IN  
SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT**

In accordance with Local Rules 7(h) and 56.1, defendant Department of Homeland Security (“DHS”) submits this concise statement of material facts as to which it contends there is no genuine issue in support of its motion for partial summary judgment on the expedited processing issue. Plaintiff also has moved for summary judgment on this issue; DHS has filed an opposition, and Local Rules 7(h) and 56.1 require that a party opposing summary judgment file “a concise statement of genuine issues setting forth all material facts as to which it is contended there exists a genuine issue necessary to be litigated.”

Local Rules 7(h) and 56.1 are somewhat inapposite in this case. Under the Freedom of Information Act (“FOIA”), review of an agency decision to deny expedited processing is based on the “record before the agency at the time of the determination.” 5 U.S.C. § 552(a)(6)(E)(iii). The record in this case consists of: (i) plaintiff’s letters to DHS requesting expedited processing of their FOIA requests, (ii) certain documents attached to these letters or referenced within the

letters, and (iii) DHS's letters denying plaintiff's requests for expedited processing. This material is attached as Exhibits A through G to plaintiff's motion for partial summary judgment. Plaintiff's Exhibits H and I are not part of the agency record and should not be considered in relation to defendant's decision to deny plaintiff's request for expedited processing.

Thus, other than certain facts relating to the legal background of the subject matter of plaintiff's requests, which are not subject to dispute, all of the facts relating to plaintiff's expedited processing claims are contained in the agency record. The documents comprising the agency record speak for themselves, and therefore are not subject to dispute or "genuine issue." Nevertheless, out of an abundance of caution, defendant submits the below statement of material facts in support of its motion, and immediately thereafter, a point-by-point response to plaintiff's statement of material facts. In responding to plaintiff's statement of material facts, defendant notes where plaintiff cites material outside the agency record.

#### DEFENDANT'S STATEMENT OF MATERIAL FACTS

1. By letter dated October 20, 2006, plaintiff submitted a FOIA request to defendant for agency records relating to the negotiation of the Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record Data ("Interim Agreement"). Plaintiff sought expedited processing of its request, and attached a one page printout of the results of a Google News search to its letter in support of this request. Plaintiff's October 20, 2006 FOIA request and its attachment are attached as Exhibit A to plaintiff's motion for partial summary judgment, which Exhibit defendant incorporates herein by reference.

2. By letter dated November 1, 2006, defendant denied plaintiff's October 20, 2006 request for expedited processing. Defendant's November 1, 2006 letter is attached as Exhibit B

to plaintiff's motion for partial summary judgment, which Exhibit defendant incorporates herein by reference.

3. By letter dated November 21, 2006, plaintiff appealed the denial of its October 20, 2006 request for expedited processing. Attached to plaintiff's letter were a copy of its latest newsletter and a copy of November 17, 2006 Reuters news article. Plaintiff's November 21, 2006 letter and its attachments are attached as Exhibit C to plaintiff's motion for partial summary judgment, which Exhibit defendant incorporates herein by reference.

4. By letter dated November 7, 2006, plaintiff submitted a FOIA request to defendant for agency records relating to the Automated Targeting System ("ATS"). Plaintiff sought expedited processing of its request. In support of its request for expedited processing plaintiff attached to its letter a one page printout of the results of a Google News search and two news articles. Plaintiff's November 7, 2006 letter and its attachments are attached as Exhibit E to plaintiff's motion for partial summary judgment, which Exhibit defendant incorporates herein by reference.

5. By letter dated December 6, 2006, plaintiff submitted another FOIA request for agency records relating to the ATS. Plaintiff also requested expedited processing of this request and attached to its letter six exhibits in support of this request. Plaintiff's December 6, 2006 letter and its attachments are attached as Exhibit F to plaintiff's motion for partial summary judgment, which Exhibit defendant incorporates herein by reference.

6. By letter dated December 14, 2006, defendant denied plaintiff's November 7, 2006 and December 6, 2006 requests for expedited processing. Defendant's December 14, 2006 letter is attached as Exhibit G to plaintiff's motion for partial summary judgment, which Exhibit

defendant incorporates herein by reference.

7. Plaintiff did not appeal the denial of its November 7, 2006 or December 6, 2006 requests for expedited processing.

RESPONSE TO PLAINTIFF'S STATEMENT OF MATERIAL FACTS

1. Paragraph 1 characterizes the Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection ("2004 Agreement"), which was referenced in plaintiff's October 20, 2006 FOIA request. A complete and accurate copy of this agreement is attached as Exhibit 1 to defendant's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of the 2004 Agreement.

2. Paragraph 2 characterizes a notice published in the Federal Register by DHS and its component the Bureau of Customs and Border Protection ("CBP"), which was referenced in plaintiff's October 20, 2006 FOIA request. The notice is entitled the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data (the "Undertakings"). Contrary to plaintiff's assertion, DHS issued the Undertakings on May 11, 2004, prior to entering into the 2004 Agreement, and published the Undertakings on July 9, 2004. A complete and accurate copy of the Undertakings is available at 69 Fed. Reg. 41,543-47 (July 9, 2004).

3. Paragraph 3 characterizes news articles that were neither attached nor referenced in plaintiff's October 20, 2006 FOIA request or its November 21, 2006 appeal of DHS's denial of its request for expedited processing. These articles were not a part of "the record before the

agency at the time of the determination” and therefore should not be considered by this Court. 5  
U.S.C. § 552(a)(6)(E)(iii).

4. Paragraph 4 characterizes a decision of the European Court of Justice (“ECJ”) issued on May 30, 2006. Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Comm’n of the European Communities*, 2006 ECJ CELEX LEXIS 239 (May 30, 2006). Plaintiff’s characterize this decision as ruling the 2004 Agreement “illegal,” implying that the ECJ found that CBP did not provide an adequate level of privacy protection in its handling of PNR data derived from flights between the EU and the U.S. In fact, the ECJ did not find that the 2004 Agreement violated the European Union’s substantive privacy law, but found that the 2004 Agreement was invalid because it was not within the competence of the European Community (“EC”) to conclude such an agreement. *Id.* at ¶ 67. A complete and accurate copy of this decision is attached as Exhibit 2 to defendant’s motion for partial summary judgment.

5. Admit.

6. Paragraph 6 characterizes the Interim Agreement. A complete and accurate copy of the Interim Agreement is available at 72 Fed. Reg. 348-49 (Jan. 4, 2007). Plaintiff’s characterization is disputed to the extent it varies with the text of the Interim Agreement.

7. Paragraph 7 characterizes the Interim Agreement, the 2004 Agreement and the judgment of the ECJ, to which the Court is respectfully referred. Plaintiff’s characterization is disputed to the extent it varies with the text of these documents.

8. Paragraph 8 characterizes a letter that accompanied the Interim Agreement. A complete and accurate copy of this letter is available at 72 Fed. Reg. 349-51 (Jan. 4, 2007).

Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

9. Paragraph 9 characterizes a letter that accompanied the Interim Agreement. A complete and accurate copy of this letter is available at 72 Fed. Reg. 349-51 (Jan. 4, 2007).

Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

10. Paragraph 10 characterizes the media attention received by the negotiation and conclusion of the Interim Agreement as "extensive." Defendant disputes this characterization.

11. Admit.

12. Paragraph 12 characterizes the systems of records notice concerning the ATS published in the Federal Register on November 7, 2006. A complete and accurate copy of this notice is available at 71 Fed. Reg. 64,543-46 (Nov. 2, 2006). Plaintiff's characterization is disputed to the extent it varies with the text of this notice.

13. Paragraph 13 characterizes the systems of records notice. A complete and accurate copy of this notice is available at 71 Fed. Reg. 64,543-46 (Nov. 2, 2006). Plaintiff's characterization is disputed to the extent it varies with the text of this notice.

14. Paragraph 14 characterizes plaintiff's October 20, 2006 FOIA request. A complete and accurate copy of plaintiff's October 20, 2006 FOIA request is attached as Exhibit A to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

15. Paragraph 15 characterizes plaintiff's October 20, 2006 FOIA request. A complete and accurate copy of plaintiff's October 20, 2006 FOIA request is attached as Exhibit A to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

16. Paragraph 16 characterizes plaintiff's October 20, 2006 FOIA request. A complete and accurate copy of plaintiff's October 20, 2006 FOIA request is attached as Exhibit A to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

17. Paragraph 17 characterizes plaintiff's October 20, 2006 FOIA request. A complete and accurate copy of plaintiff's October 20, 2006 FOIA request is attached as Exhibit A to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

18. Paragraph 18 characterizes defendant's November 1, 2006 letter denying plaintiff's October 20, 2006 request for expedited processing. A complete and accurate copy of defendant's November 1, 2006 letter is attached as Exhibit B to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

19. Paragraph 19 characterizes defendant's November 1, 2006 letter denying plaintiff's October 20, 2006 request for expedited processing. A complete and accurate copy of defendant's November 1, 2006 letter is attached as Exhibit B to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

20. Paragraph 20 characterizes plaintiff's November 21, 2006 letter appealing the denial of plaintiff's October 20, 2006 request for expedited processing. A complete and accurate copy of plaintiff's November 21, 2006 letter is attached as Exhibit C to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the

text of this letter.

21. Paragraph 21 characterizes plaintiff's November 21, 2006 letter appealing the denial of plaintiff's October 20, 2006 request for expedited processing. A complete and accurate copy of plaintiff's November 21, 2006 letter is attached as Exhibit C to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

22. Paragraph 22 characterizes plaintiff's initial complaint in Civil Action 06-1988, to which the Court is respectfully referred for a full and complete understanding of its contents.

23. Paragraph 23 characterizes plaintiff's amended complaint in Civil Action 06-1988, to which the Court is respectfully referred for a full and complete understanding of its contents.

24. Paragraph 24 characterizes plaintiff's November 7, 2006 and December 6, 2006 FOIA requests. Complete and accurate copies of these requests are attached as Exhibits E and F to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of these requests.

25. Paragraph 25 characterizes plaintiff's November 7, 2006 and December 6, 2006 FOIA requests. Complete and accurate copies of these requests are attached as Exhibits E and F to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of these requests.

26. Paragraph 26 characterizes plaintiff's October 20, 2006, November 7, 2006 and December 6, 2006 FOIA requests. Complete and accurate copies of these requests are attached as Exhibits A, E and F to plaintiff's motion for partial summary judgment. Plaintiff's

characterization is disputed to the extent it varies with the text of these requests.

27. Paragraph 27 characterizes plaintiff's November 7, 2006 FOIA request. A complete and accurate copy of this requests is attached as Exhibit E to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

28. Paragraph 28 characterizes plaintiff's December 6, 2006 FOIA request. A complete and accurate copy of this requests is attached as Exhibit F to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

29. Paragraph 29 characterizes plaintiff's December 6, 2006 FOIA request. A complete and accurate copy of this request is attached as Exhibit F to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this request.

30. Paragraph 30 characterizes defendant's December 14, 2006 letter denying plaintiff's request for expedited processing. A complete and accurate copy of this letter is attached as Exhibit G to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

31. Paragraph 31 characterizes defendant's December 14, 2006 letter denying plaintiff's request for expedited processing. A complete and accurate copy of this letter is attached as Exhibit G to plaintiff's motion for partial summary judgment. Plaintiff's characterization is disputed to the extent it varies with the text of this letter.

32. Paragraph 32 characterizes plaintiff's initial complaint in Civil Action 06-2154, to

which the Court is respectfully referred for a full and complete understanding of its contents.

Dated: February 22, 2007

Respectfully Submitted,

PETER D. KEISLER  
Assistant Attorney General

JEFFREY A. TAYLOR  
United States Attorney

ELIZABETH J. SHAPIRO  
(D.C. Bar 418925)  
Assistant Branch Director  
U.S. Department of Justice  
Civil Division, Federal Programs Branch

/s/ John R. Coleman  
JOHN R. COLEMAN  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
Mailing Address  
P.O. Box 883  
Washington, D.C., 20044  
Delivery Address  
20 Massachusetts Avenue, NW, Room 6118  
Washington, D.C. 20530  
Telephone: (202) 514-4505  
Facsimile: (202) 616-8187  
john.coleman3

/s/ Adam D Kirschner  
ADAM D. KIRSCHNER  
Trial Attorney  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
Mailing Address  
P.O. Box 883  
Washington, D.C., 20044  
Delivery Address

20 Massachusetts Avenue, NW, Room 7126  
Washington, D.C. 20530  
Telephone: (202) 353-9265  
Fax: (202) 616-8470  
adam.kirschner@usdoj.gov

Counsel for Defendant

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC FRONTIER FOUNDATION )

Plaintiff, )

v. )

DEPARTMENT OF HOMELAND SECURITY )

Defendant. )

Consolidated Cases

Civil Action No. 06-1988 (ESH)

Civil Action No. 06-2154 (RBW)

DECLARATION OF JOHN R. COLEMAN

I, JOHN R. COLEMAN, do hereby state and declare as follows:

1. I am a trial attorney for the Department of Justice, Civil Division, Federal Programs Branch, and have been a trial attorney since October 2, 2006. I am lead counsel for defendants in Civil Action No. 06-1988. I submit this declaration in support of Defendant's Motion for Partial Summary Judgment and Defendant's Opposition to Plaintiff's Motion for Partial Summary Judgment. The statements herein are based on my personal knowledge and information obtained in the course of my official duties.

2. Exhibit 1 is a true and correct copy of the Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, signed May 28, 2004 (the "2004 Agreement").

3. Exhibit 2 is a true and correct copy of the opinion of the European Court of Justice in Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Comm'n of the European Communities*, 2006 ECJ CELEX LEXIS 239

(May 30, 2006).

4. Exhibit 3 is a true and correct copy of the November 22, 2006 Privacy Impact Assessment of the Automated Targeting System.

5. Exhibit 4 is a true and accurate copy of a November 14, 2006 letter to David Sobel of the Electronic Frontier Foundation from Catherine Papoi, Deputy Chief FOIA Office, and Director, Disclosure & FOIA of the Department of Homeland Security.

6. Exhibit 5 is a true and accurate copy of the "About EFF" web page that I downloaded from the website of the Electronic Frontier Foundation, [www.eff.org](http://www.eff.org), on February 19, 2007.

7. Exhibit 6 is a true and accurate copy of a Guidestar Basic Report for the Electronic Frontier Foundation, cited in plaintiff's requests, that I downloaded from [www.guidestar.org](http://www.guidestar.org) on February 21, 2007.

8. Exhibit 7 is a true and accurate copy of a Google News search conducted by me on February 16, 2007 using the search term "Iran and Nuclear and 'United States.'"

9. Exhibit 8 is a true and accurate copy of a Google News search conducted by me on February 16, 2007 using the search term "Surge and Iraq"

10. Exhibit 9 is a true and accurate copy of a Google News search conducted by me on February 16, 2007 with the search term "cricket and match."

11. Exhibit 10 is a true and accurate copy of a press roundtable conducted on December 12, 2006 by Daniel Fried, Assistant Secretary for European and Eurasian Affairs, of the United States Department of State that I downloaded on February 16, 2007. These remarks are available at the Department of State's website, <http://www.state.gov/p/eur/rls/rm/77854.htm>.

12. Exhibit 11 is a true and accurate copy of the Source Information for the Major

Newspapers database within Lexis-Nexis, which I downloaded and printed from the Lexis-Nexis website on February 21, 2007.

13. Exhibit 12 is a true and accurate copy of the search results of a search for the term "Automated Targeting System" for the period November 1, 2006 to December 14, 2006. This search was conducted by me on February 21, 2006 within the Lexis-Nexis Major Newspapers database.

I declare under penalty of perjury that the foregoing is true and correct.

Date: February 22, 2007



JOHN R. COLEMAN

**Exhibit 1**

***Defendant's Motion for Partial Summary Judgment***

AGREEMENT  
BETWEEN THE EUROPEAN COMMUNITY AND  
THE UNITED STATES OF AMERICA  
ON THE PROCESSING AND TRANSFER OF PNR DATA BY AIR CARRIERS  
TO THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY,  
BUREAU OF CUSTOMS AND BORDER PROTECTION

CE/USA/en 1

THE EUROPEAN COMMUNITY AND THE UNITED STATES OF AMERICA,

RECOGNISING the importance of respecting fundamental rights and freedoms, notably privacy, and the importance of respecting these values, while preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime,

HAVING REGARD to U.S. statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide the Department of Homeland Security (hereinafter "DHS"), Bureau of Customs and Border Protection (hereinafter "CBP") with electronic access to Passenger Name Record (hereinafter "PNR") data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems,

HAVING REGARD to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and in particular Article 7(c) thereof,

HAVING REGARD to the Undertakings of CBP issued on 11 May 2004, which will be published in the Federal Register (hereinafter "the Undertakings"),

HAVING REGARD to Commission Decision C (2004) 1914 adopted on 14 May 2004, pursuant to Article 25(6) of Directive 95/46/EC, whereby CBP is considered as providing an adequate level of protection for PNR data transferred from the European Community (hereinafter "Community") concerning flights to or from the U.S. in accordance with the Undertakings, which are annexed thereto (hereinafter "the Decision"),

NOTING that air carriers with reservation/departure control systems located within the territory of the Member States of the European Community should arrange for transmission of PNR data to CBP as soon as this is technically feasible but that, until then, the U.S. authorities should be allowed to access the data directly, in accordance with the provisions of this Agreement,

AFFIRMING that this Agreement does not constitute a precedent for any future discussions and negotiations between the United States and the European Community, or between either of the Parties and any State regarding the transfer of any other form of data,

HAVING REGARD to the commitment of both sides to work together to reach an appropriate and mutually satisfactory solution, without delay, on the processing of Advance Passenger Information (API) data from the Community to the U.S.,

HAVE AGREED AS FOLLOWS:

- 1) CBP may electronically access the PNR data from air carriers' reservation/departure control systems ("reservation systems") located within the territory of the Member States of the European Community strictly in accordance with the Decision and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers.
  
- 2) Air carriers operating passenger flights in foreign air transportation to or from the United States shall process PNR data contained in their automated reservation systems as required by CBP pursuant to U.S. law and strictly in accordance with the Decision and for so long as the Decision is applicable.
  
- 3) CBP takes note of the Decision and states that it is implementing the Undertakings annexed thereto.
  
- 4) CBP shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable U.S. laws and constitutional requirements, without unlawful discrimination, in particular on the basis of nationality and country of residence.

5) CBP and the European Commission shall jointly and regularly review the implementation of this Agreement.

6) In the event that an airline passenger identification system is implemented in the European Union which requires air carriers to provide authorities with access to PNR data for persons whose current travel itinerary includes a flight to or from the European Union, DHS shall, in so far as practicable and strictly on the basis of reciprocity, actively promote the cooperation of airlines within its jurisdiction.

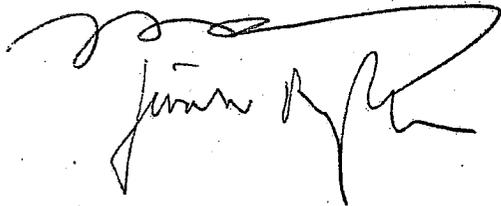
7) This Agreement shall enter into force upon signature. Either Party may terminate this Agreement at any time by notification through diplomatic channels. The termination shall take effect ninety (90) days from the date of notification of termination to the other Party. This Agreement may be amended at any time by mutual written agreement.

- 8) This Agreement is not intended to derogate from or amend legislation of the Parties; nor does this Agreement create or confer any right or benefit on any other person or entity, private or public.

Signed at Washington D.C. on the twenty-eighth day of May in the year two thousand and four.

This Agreement is drawn up in duplicate in the Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Slovak, Slovenian, Spanish and Swedish languages, each text being equally authentic. In case of divergence, the English version shall prevail.

Por la Comunidad Europea  
Za Evropské společenství  
For Det Europæiske Fællesskab  
Für die Europäische Gemeinschaft  
Euroopa Ühenduse nimel  
Για την Ευρωπαϊκή Κοινότητα  
For the European Community  
Pour la Communauté européenne  
Per la Comunità europea  
Eiropas Kopienas vārdā  
Europos bendrijos vardu  
az Európai Közösség részéről  
Għall-Komunità Ewropea  
Voor de Europese Gemeenschap  
W imieniu Wspólnoty Europejskiej  
Pela Comunidade Europeia  
Za Európske spoločenstvo  
za Evropsko skupnost  
Euroopan yhteisön puolesta  
På Europeiska gemenskapens vägnar



Por los Estados Unidos de América  
Za Spojené státy americké  
For Amerikas Forenede Stater  
Für die Vereinigten Staaten von Amerika  
Ameerika Ühendriikide nimel  
Για τις Ηνωμένες Πολιτείες της Αμερικής  
For the United States of America  
Pour les Etats-Unis d'Amérique  
Per gli Stati Uniti d'America  
Amerikas Savienoto Valstu vārdā  
Jungtinių Amerikos Valstijų vardu  
az Amerikai Egyesült Államok részéről  
Għall-Istati Uniti ta' l-Amerika  
Voor de Verenigde Staten van Amerika  
W imieniu Stanów Zjednoczonych Ameryki  
Pelos Estados Unidos da América  
Za Spojené štáty americké  
Za Združene države Amerike  
Amerikan yhdysvaltojen puolesta  
På Amerikas förenta staters vägnar



**Exhibit 2**

***Defendant's Motion for Partial Summary Judgment***

**IMPORTANT LEGAL NOTICE** - The information on this site is subject to a disclaimer and a copyright notice.

JUDGMENT OF THE COURT (Grand Chamber)

30 May 2006 (\*)

(Protection of individuals with regard to the processing of personal data – Air transport – Decision 2004/496/EC – Agreement between the European Community and the United States of America – Passenger Name Records of air passengers transferred to the United States Bureau of Customs and Border Protection – Directive 95/46/EC – Article 25 – Third countries – Decision 2004/535/EC – Adequate level of protection)

In Joined Cases C-317/04 and C-318/04,

ACTIONS for annulment under Article 230 EC, brought on 27 July 2004,

**European Parliament**, represented by R. Passos, N. Lorenz, H. Duintjer Tebbens and A. Caiola, acting as Agents, with an address for service in Luxembourg,

applicant,

supported by:

**European Data Protection Supervisor (EDPS)**, represented by H. Hijmans and V. Perez Asinari, acting as Agents,

intervener,

v

**Council of the European Union**, represented by M.C. Giorgi Fort and M. Bishop, acting as Agents,

defendant in Case C-317/04,

supported by:

**Commission of the European Communities**, represented by P.J. Kuijper, A. van Solinge and C. Docksey, acting as Agents, with an address for service in Luxembourg,

**United Kingdom of Great Britain and Northern Ireland**, represented by M. Bethell, C. White and T. Harris, acting as Agents, and T. Ward, Barrister, with an address for service in Luxembourg,

interveners,

and v

**Commission of the European Communities**, represented by P.J. Kuijper, A. van Solinge, C. Docksey and F. Benyon, acting as Agents, with an address for service in Luxembourg,

defendant in Case C-318/04,

supported by:

**United Kingdom of Great Britain and Northern Ireland**, represented by M. Bethell, C. White and T. Harris, acting as Agents, and T. Ward, Barrister, with an address for service in Luxembourg,

intervener,

THE COURT (Grand Chamber),

composed of V. Skouris, President, P. Jann, C.W.A. Timmermans, A. Rosas and J. Malenovský, Presidents of Chambers, N. Colneric (Rapporteur), S. von Bahr, J.N. Cunha Rodrigues, R. Silva de Lapuerta, G. Arestis, A. Borg Barthet, M. Ilešič and J. Klučka, Judges,

Advocate General: P. Léger,

Registrar: M. Ferreira, Principal Administrator,

having regard to the written procedure and further to the hearing on 18 October 2005,

after hearing the Opinion of the Advocate General at the sitting on 22 November 2005,

gives the following

#### Judgment

- 1 By its application in Case C-317/04, the European Parliament seeks the annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004 L 183, p. 83, and corrigendum at OJ 2005 L 255, p. 168).
- 2 By its application in Case C-318/04, the Parliament seeks the annulment of Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection (OJ 2004 L 235, p. 11; hereinafter 'the decision on adequacy').

#### Legal context

- 3 Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (hereinafter 'the ECHR'), provides:
  1. Everyone has the right to respect for his private and family life, his home and his correspondence.
  2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'
- 4 The second sentence of Article 95(1) EC is worded as follows:

'The Council shall, acting in accordance with the procedure referred to in Article 251 and after consulting the Economic and Social Committee, adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market.'
- 5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 adapting to Council Decision 1999/468/EC the provisions relating to committees which assist the Commission in the exercise of its implementing powers laid down in instruments subject to the procedure referred to in Article 251 of the EC Treaty (OJ 2003 L 284, p. 1) (hereinafter 'the Directive'), was adopted on the basis of Article 100a of the EC Treaty (now, after amendment, Article 95 EC).
- 6 The 11th recital in the preamble to the Directive states that 'the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data'.
- 7 The 13th recital in the preamble reads as follows:

'... the activities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the activities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56(2), Article 57 or Article 100a of the Treaty establishing the European Community ...'.
- 8 The 57th recital states:

'... the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited'.

9 Article 2 of the Directive provides:

'For the purposes of this Directive:

- (a) "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
- (b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

10 Article 3 of the Directive is worded as follows:

'Scope

- 1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
- 2. This Directive shall not apply to the processing of personal data:
  - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

...

11 Article 6(1) of the Directive states:

'Member States shall provide that personal data must be:

...

- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- ...
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. ...'

12 Article 7 of the Directive provides:

'Member States shall provide that personal data may be processed only if:

...

- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- ...
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

13 The first subparagraph of Article 8(5) of the Directive is worded as follows:

'Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.'

14 Article 12 of the Directive provides:

'Member States shall guarantee every data subject the right to obtain from the controller:

- (a) without constraint at reasonable intervals and without excessive delay or expense:
  - confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
  - communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
  - knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);
- (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
- (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.'

15 Article 13(1) of the Directive is worded as follows:

'Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary [measure] to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.'

16 Article 22 of the Directive provides:

'Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.'

17 Articles 25 and 26 of the Directive constitute Chapter IV, on the transfer of personal data to third countries.

18 Article 25, headed 'Principles', provides:

'1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be

given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.'

19 Article 26(1) of the Directive, under the heading 'Derogations', is worded as follows:

'By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2) may take place on condition that:

- (a) the data subject has given his consent unambiguously to the proposed transfer; or
- (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- (e) the transfer is necessary in order to protect the vital interests of the data subject; or
- (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.'

20 It was on the basis of the Directive, in particular Article 25(6) thereof, that the Commission of the European Communities adopted the decision on adequacy.

21 The 11th recital in the preamble to that decision states:

'The processing by CBP [the Bureau of Customs and Border Protection] of personal data contained in the PNR [Passenger Name Record] of air passengers transferred to it is governed by conditions set out in the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) of 11 May 2004 (hereinafter referred to as the Undertakings) and in United States domestic legislation to the extent indicated in the Undertakings.'

22 The 15th recital in the preamble to the decision states that PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious crimes, including organised crime, that are transnational in nature, and flight from warrants or custody for those crimes.

23 Articles 1 to 4 of the decision on adequacy provide:

*Article 1*

For the purposes of Article 25(2) of Directive 95/46/EC, the United States Bureau of Customs and Border Protection (hereinafter referred to as CBP) is considered to ensure an adequate level of protection for PNR data transferred from the Community concerning flights to or from the United States, in accordance with the Undertakings set out in the Annex.

*Article 2*

This Decision concerns the adequacy of protection provided by CBP with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and shall not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States.

*Article 3*

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to CBP in order to protect individuals with regard to the processing of their personal data in the following cases:

- (a) where a competent United States authority has determined that CBP is in breach of the applicable standards of protection; or
- (b) where there is a substantial likelihood that the standards of protection set out in the Annex are being infringed, there are reasonable grounds for believing that CBP is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects, and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide CBP with notice and an opportunity to respond.

2. Suspension shall cease as soon as the standards of protection are assured and the competent authorities of the Member States concerned are notified thereof.

*Article 4*

1. Member States shall inform the Commission without delay when measures are adopted pursuant to Article 3.

2. The Member States and the Commission shall inform each other of any changes in the standards of protection and of cases where the action of bodies responsible for ensuring compliance with the standards of protection by CBP as set out in the Annex fails to secure such compliance.

3. If the information collected pursuant to Article 3 and pursuant to paragraphs 1 and 2 of this Article provides evidence that the basic principles necessary for an adequate level of protection for natural persons are no longer being complied with, or that any body responsible for ensuring compliance with the standards of protection by CBP as set out in the Annex is not effectively fulfilling its role, CBP shall be informed and, if necessary, the procedure referred to in Article 31(2) of Directive 95/46/EC shall apply with a view to repealing or suspending this Decision.

24 The Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection (CBP) annexed to the decision on adequacy state:

'In support of the plan of the European Commission (Commission) to exercise the powers conferred on it by Article 25(6) of Directive 95/46/EC ... and to adopt a decision recognising the Department of Homeland Security Bureau of Customs and Border Protection (CBP) as providing adequate protection for the purposes of air carrier transfers of [PNR] data which may fall within the scope of the Directive, CBP undertakes as follows ...'

25 The Undertakings comprise 48 paragraphs, arranged under the following headings: 'Legal authority to obtain PNR'; 'Use of PNR data by CBP'; 'Data requirements'; 'Treatment of "sensitive" data'; 'Method of accessing PNR data'; 'Storage of PNR data'; 'CBP computer system security'; 'CBP treatment and protection of PNR data'; 'Transfer of PNR data to other government authorities'; 'Notice, access and opportunities for redress for PNR data subjects'; 'Compliance issues'; 'Reciprocity'; 'Review and termination of Undertakings'; and 'No private right or precedent created'.

26 The Undertakings include the following:

'1. By legal statute (title 49, United States Code, section 44909(c)(3)) and its implementing (interim) regulations (title 19, Code of Federal Regulations, section 122.49b), each air carrier operating passenger flights in foreign air transportation to or from the United States, must provide CBP (formerly, the US Customs Service) with electronic access to PNR data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems (reservation systems).

...

3. PNR data are used by CBP strictly for purposes of preventing and combating: 1. terrorism and related crimes; 2. other serious crimes, including organised crime, that are transnational in nature; and 3. flight from warrants or custody for the crimes described above. Use of PNR data for these purposes permits CBP to focus its resources on high-risk concerns, thereby facilitating and safeguarding bona fide travel.

4. Data elements which CBP require are listed herein at Attachment A. ...

...

27. CBP will take the position in connection with any administrative or judicial proceeding arising out of a FOIA [Freedom of Information Act] request for PNR information accessed from air carriers, that such records are exempt from disclosure under the FOIA.
- ...
29. CBP, in its discretion, will only provide PNR data to other government authorities, including foreign government authorities, with counter-terrorism or law-enforcement functions, on a case-by-case basis, for purposes of preventing and combating offences identified in paragraph 3 herein. (Authorities with whom CBP may share such data shall hereinafter be referred to as the Designated Authorities).
30. CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes. CBP will first determine if the reason for disclosing the PNR data to another Designated Authority fits within the stated purpose (see paragraph 29 herein). If so, CBP will determine whether that Designated Authority is responsible for preventing, investigating or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose, where CBP is aware of an indication of a violation or potential violation of law. The merits of disclosure will need to be reviewed in light of all the circumstances presented.
- ...
35. No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law. CBP will advise the European Commission regarding the passage of any US legislation which materially affects the statements made in these Undertakings.
- ...
46. These Undertakings shall apply for a term of three years and six months (3.5 years), beginning on the date upon which an agreement enters into force between the United States and the European Community, authorising the processing of PNR data by air carriers for purposes of transferring such data to CBP, in accordance with the Directive. ...
47. These Undertakings do not create or confer any right or benefit on any person or party, private or public.
- ...
27. Attachment A to the Undertakings contains the 'PNR data elements' required by CBP from air carriers. The PNR data elements include the 'PNR record locator code', date of reservation, name, address, all forms of payment information, contact telephone numbers, travel agency, travel status of the passenger, e-mail address, general remarks, seat number, no-show history and any collected APIS (Advanced Passenger Information System) information.
28. The Council adopted Decision 2004/496 on the basis, in particular, of Article 95 EC in conjunction with the first sentence of the first subparagraph of Article 300(2) EC.
29. The three recitals in the preamble to that decision state:
- '(1) On 23 February 2004 the Council authorised the Commission to negotiate, on behalf of the Community, an Agreement with the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection.
- (2) The European Parliament has not given an Opinion within the time-limit which, pursuant to the first subparagraph of Article 300(3) of the Treaty, the Council laid down in view of the urgent need to remedy the situation of uncertainty in which airlines and passengers found themselves, as well as to protect the financial interests of those concerned.
- (3) This Agreement should be approved.'
30. Article 1 of Decision 2004/496 provides:
- 'The Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection is hereby approved on behalf of the Community.
- The text of the Agreement is attached to this Decision.'
31. That agreement (hereinafter 'the Agreement') is worded as follows:
- 'The European Community and the United States of America,

Recognising the importance of respecting fundamental rights and freedoms, notably privacy, and the importance of respecting these values, while preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime,

Having regard to US statutes and regulations requiring each air carrier operating passenger flights in foreign air transportation to or from the United States to provide the Department of Homeland Security (hereinafter "DHS"), Bureau of Customs and Border Protection (hereinafter "CBP") with electronic access to Passenger Name Record (hereinafter "PNR") data to the extent it is collected and contained in the air carrier's automated reservation/departure control systems,

Having regard to Directive 95/46/EC ..., and in particular Article 7(c) thereof,

Having regard to the Undertakings of CBP issued on 11 May 2004, which will be published in the Federal Register (hereinafter "the Undertakings"),

Having regard to Commission Decision 2004/535/EC adopted on 14 May 2004, pursuant to Article 25(6) of Directive 95/46/EC, whereby CBP is considered as providing an adequate level of protection for PNR data transferred from the European Community (hereinafter "Community") concerning flights to or from the US in accordance with the Undertakings, which are annexed thereto (hereinafter "the Decision"),

Noting that air carriers with reservation/departure control systems located within the territory of the Member States of the European Community should arrange for transmission of PNR data to CBP as soon as this is technically feasible but that, until then, the US authorities should be allowed to access the data directly, in accordance with the provisions of this Agreement,

...

Have agreed as follows:

- (1) CBP may electronically access the PNR data from air carriers' reservation/departure control systems ("reservation systems") located within the territory of the Member States of the European Community strictly in accordance with the Decision and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers.
- (2) Air carriers operating passenger flights in foreign air transportation to or from the United States shall process PNR data contained in their automated reservation systems as required by CBP pursuant to US law and strictly in accordance with the Decision and for so long as the Decision is applicable.
- (3) CBP takes note of the Decision and states that it is implementing the Undertakings annexed thereto.
- (4) CBP shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable US laws and constitutional requirements, without unlawful discrimination, in particular on the basis of nationality and country of residence.
- ...
- (7) This Agreement shall enter into force upon signature. Either Party may terminate this Agreement at any time by notification through diplomatic channels. The termination shall take effect ninety (90) days from the date of notification of termination to the other Party. This Agreement may be amended at any time by mutual written agreement.
- (8) This Agreement is not intended to derogate from or amend legislation of the Parties; nor does this Agreement create or confer any right or benefit on any other person or entity, private or public.

- 32 According to Council information concerning the date of its entry into force (OJ 2004 C 158, p. 1), the Agreement, signed in Washington on 28 May 2004 by a representative of the Presidency-in-Office of the Council and the Secretary of the United States Department of Homeland Security, entered into force on the date of its signature, as provided by paragraph 7 of the Agreement.

#### Background

- 33 Following the terrorist attacks of 11 September 2001, the United States passed legislation in November 2001 providing that air carriers operating flights to or from the United States or across United States territory had to provide the United States customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' (hereinafter 'PNR data'). While acknowledging the legitimacy of the security interests at stake, the Commission informed the United States authorities, in June 2002, that those provisions could come into conflict with Community and Member State legislation on data protection and with certain provisions of Council Regulation (EEC) No 2299/89 of 24 July 1989 on a code of conduct for computerised reservation systems (OJ 1989 L 220, p. 1), as amended by Council Regulation (EC) No 323/1999 of 8 February 1999 (OJ 1999 L 40, p. 1). The United States authorities postponed the entry into force of the new provisions but, ultimately, refused to waive the right to impose penalties on airlines failing to comply with the legislation on electronic access to PNR data

after 5 March 2003. Since then, a number of large airlines in the European Union have granted the United States authorities access to their PNR data.

- 34 The Commission entered into negotiations with the United States authorities, which gave rise to a document containing undertakings on the part of CBP, with a view to the adoption by the Commission of a decision on adequacy pursuant to Article 25(6) of the Directive.
- 35 On 13 June 2003 the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, set up by Article 29 of the Directive, delivered an opinion in which it expressed doubts regarding the level of data protection guaranteed by those undertakings for the processing operations envisaged. It reiterated those doubts in an opinion of 29 January 2004.
- 36 On 1 March 2004 the Commission placed before the Parliament the draft decision on adequacy under Article 25(6) of the Directive, together with the draft undertakings of CBP.
- 37 On 17 March 2004 the Commission submitted to the Parliament, with a view to its consultation in accordance with the first subparagraph of Article 300(3) EC, a proposal for a Council decision concerning the conclusion of an agreement with the United States. By letter of 25 March 2004, the Council, referring to the urgent procedure, requested the Parliament to deliver an opinion on that proposal by 22 April 2004 at the latest. In that letter, the Council stated: 'The fight against terrorism, which justifies the proposed measures, is a key priority of the European Union. Air carriers and passengers are at present in a situation of uncertainty which urgently needs to be remedied. In addition, it is essential to protect the financial interests of the parties concerned.'
- 38 On 31 March 2004 the Parliament, acting pursuant to Article 8 of Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (OJ 1999 L 184, p. 23), adopted a resolution setting out a number of reservations of a legal nature regarding the proposal which had been submitted to it. In particular, the Parliament considered that the draft decision on adequacy exceeded the powers conferred on the Commission by Article 25 of the Directive. It called for the conclusion of an appropriate international agreement respecting fundamental rights that would cover a number of points set out in detail in the resolution, and asked the Commission to submit a new draft decision to it. It also reserved the right to refer the matter to the Court for review of the legality of the projected international agreement and, in particular, of its compatibility with protection of the right to privacy.
- 39 On 21 April 2004 the Parliament, at the request of its President, approved a recommendation from the Committee on Legal Affairs and the Internal Market that, in accordance with Article 300(6) EC, an Opinion be obtained from the Court on the compatibility of the agreement envisaged with the Treaty. That procedure was initiated on that very day.
- 40 The Parliament also decided, on the same day, to refer to committee the report on the proposal for a Council decision, thus implicitly rejecting, at that stage, the Council's request of 25 March 2004 for urgent consideration of the proposal.
- 41 On 28 April 2004 the Council, acting on the basis of the first subparagraph of Article 300(3) EC, sent a letter to the Parliament asking it to deliver its opinion on the proposal for a decision relating to the conclusion of the Agreement by 5 May 2004. To justify the urgency of that request, the Council restated the reasons set out in its letter of 25 March 2004.
- 42 After taking note of the continuing lack of all the language versions of the proposal for a Council decision, on 4 May 2004 the Parliament rejected the Council's request to it of 28 April for urgent consideration of that proposal.
- 43 On 14 May 2004 the Commission adopted the decision on adequacy, which is the subject of Case C-318/04. On 17 May 2004 the Council adopted Decision 2004/496, which is the subject of Case C-317/04.
- 44 By letter of 4 June 2004, the Presidency-in-Office of the Council informed the Parliament that Decision 2004/496 took into account the fight against terrorism – a priority of the Union – but also the need to address the uncertain legal situation of air carriers as well as their financial interests.
- 45 By letter of 9 July 2004, the Parliament informed the Court of the withdrawal of its request for an Opinion, which had been registered under No 1/04.
- 46 In Case C-317/04, the Commission and the United Kingdom of Great Britain and Northern Ireland were granted leave to intervene in support of the form of order sought by the Council, by orders of the President of the Court of 18 November 2004 and 18 January 2005.
- 47 In Case C-318/04, the United Kingdom was granted leave to intervene in support of the form of order sought by the Commission, by order of the President of the Court of 17 December 2004.
- 48 By orders of the Court of 17 March 2005, the European Data Protection Supervisor was granted leave to intervene in support of the form of order sought by the Parliament in both cases.

- 49 Given the connection, confirmed at the hearing, between the cases, it is appropriate to join them under Article 43 of the Rules of Procedure for the purposes of the judgment.

**The application in Case C-318/04**

- 50 The Parliament advances four pleas for annulment, alleging, respectively, *ultra vires* action, breach of the fundamental principles of the Directive, breach of fundamental rights and breach of the principle of proportionality.

*The first limb of the first plea: breach of the first indent of Article 3(2) of the Directive*

Arguments of the parties

- 51 The Parliament contends that adoption of the Commission decision was *ultra vires* because the provisions laid down in the Directive were not complied with; in particular, the first indent of Article 3(2) of the Directive, relating to the exclusion of activities which fall outside the scope of Community law, was infringed.

- 52 In the Parliament's submission, there is no doubt that the processing of PNR data after transfer to the United States authority covered by the decision on adequacy is, and will be, carried out in the course of activities of the State as referred to in paragraph 43 of the judgment in Case C-101/01 *Lindqvist* [2003] ECR I-12971.

- 53 The Commission, supported by the United Kingdom, considers that the air carriers' activities clearly fall within the scope of Community law. It submits that those private operators process the PNR data within the Community and arrange for their transfer to a third country. Activities of private parties are therefore involved, and not activities of the Member State in which the carriers concerned operate, or of its public authorities, as defined by the Court in paragraph 43 of *Lindqvist*. The aim pursued by the air carriers in processing PNR data is simply to comply with the requirements of Community law, including the obligation laid down in paragraph 2 of the Agreement. Article 3(2) of the Directive refers to activities of public authorities which fall outside the scope of Community law.

Findings of the Court

- 54 The first indent of Article 3(2) of the Directive excludes from the Directive's scope the processing of personal data in the course of an activity which falls outside the scope of Community law, such as activities provided for by Titles V and VI of the Treaty on European Union, and in any case processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

- 55 The decision on adequacy concerns only PNR data transferred to CBP. It is apparent from the sixth recital in the preamble to the decision that the requirements for that transfer are based on a statute enacted by the United States in November 2001 and on implementing regulations adopted by CBP under that statute. According to the seventh recital in the preamble, the United States legislation in question concerns the enhancement of security and the conditions under which persons may enter and leave the country. The eighth recital states that the Community is fully committed to supporting the United States in the fight against terrorism within the limits imposed by Community law. The 15th recital states that PNR data will be used strictly for purposes of preventing and combating terrorism and related crimes, other serious crimes, including organised crime, that are transnational in nature, and flight from warrants or custody for those crimes.

- 56 It follows that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law.

- 57 While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite different in nature. As pointed out in paragraph 55 of the present judgment, that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes.

- 58 The Court held in paragraph 43 of *Lindqvist*, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are, in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR data have been collected by private operators for commercial purposes and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. The transfer falls within a framework established by the public authorities that relates to public security.

- 59 It follows from the foregoing considerations that the decision on adequacy concerns processing of personal data as referred to in the first indent of Article 3(2) of the Directive. That decision therefore does not fall within the scope of the Directive.

60 Accordingly, the first limb of the first plea, alleging that the first indent of Article 3(2) of the Directive was infringed, is well founded.

61 The decision on adequacy must consequently be annulled and it is not necessary to consider the other limbs of the first plea or the other pleas relied upon by the Parliament.

**The application in Case C-317/04**

62 The Parliament advances six pleas for annulment, concerning the incorrect choice of Article 95 EC as legal basis for Decision 2004/496 and breach of, respectively, the second subparagraph of Article 300(3) EC, Article 8 of the ECHR, the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith.

*The first plea: incorrect choice of Article 95 EC as legal basis for Decision 2004/496*

**Arguments of the parties**

63 The Parliament submits that Article 95 EC does not constitute an appropriate legal basis for Decision 2004/496. The decision does not have as its objective and subject-matter the establishment and functioning of the internal market by contributing to the removal of obstacles to the freedom to provide services and it does not contain provisions designed to achieve such an objective. Its purpose is to make lawful the processing of personal data that is required by United States legislation. Nor can Article 95 EC justify Community competence to conclude the Agreement, because the Agreement relates to data processing operations which are excluded from the scope of the Directive.

64 The Council contends that the Directive, validly adopted on the basis of Article 100a of the Treaty, contains in Article 25 provisions enabling personal data to be transferred to a third country which ensures an adequate level of protection, including the possibility of entering, if need be, into negotiations leading to the conclusion by the Community of an agreement with that country. The Agreement concerns the free movement of PNR data between the Community and the United States under conditions which respect the fundamental freedoms and rights of individuals, in particular privacy. It is intended to eliminate any distortion of competition, between the Member States' airlines and between the latter and the airlines of third countries, which may result from the requirements imposed by the United States, for reasons relating to the protection of individual rights and freedoms. The conditions of competition between Member States' airlines operating international passenger flights to and from the United States could have been distorted because only some of them granted the United States authorities access to their databases. The Agreement is designed to impose harmonised obligations on all the airlines concerned.

65 The Commission observes that there is a 'conflict of laws', within the meaning of public international law, between the United States legislation and the Community rules and that it is necessary to reconcile them. It complains that the Parliament, which disputes that Article 95 EC can constitute the legal basis for Decision 2004/496, has not suggested an appropriate legal basis. According to the Commission, that article is 'the natural legal basis' for the decision because the Agreement concerns the external dimension of the protection of personal data when transferred within the Community. Articles 25 and 26 of the Directive justify exclusive Community external competence.

66 In addition, the Commission submits that the initial processing of the data by the airlines is carried out for commercial purposes. The use which the United States authorities make of the data does not remove them from the effect of the Directive.

**Findings of the Court**

67 Article 95 EC, read in conjunction with Article 25 of the Directive, cannot justify Community competence to conclude the Agreement.

68 The Agreement relates to the same transfer of data as the decision on adequacy and therefore to data processing operations which, as has been stated above, are excluded from the scope of the Directive.

69 Consequently, Decision 2004/496 cannot have been validly adopted on the basis of Article 95 EC.

70 That decision must therefore be annulled and it is not necessary to consider the other pleas relied upon by the Parliament.

**Limitation of the effects of the judgment**

71 Under paragraph 7 of the Agreement, either party may terminate the Agreement at any time and the termination takes effect 90 days from the date of notification of termination to the other party.

- 72 However, in accordance with paragraphs 1 and 2 of the Agreement, CBP's right of access to PNR data and the obligation imposed on air carriers to process them as required by CBP exist only for so long as the decision on adequacy is applicable. In paragraph 3 of the Agreement, CBP stated that it was implementing the Undertakings annexed to that decision.
- 73 Given, first, the fact that the Community cannot rely on its own law as justification for not fulfilling the Agreement which remains applicable during the period of 90 days from termination thereof and, second, the close link that exists between the Agreement and the decision on adequacy, it appears justified, for reasons of legal certainty and in order to protect the persons concerned, to preserve the effect of the decision on adequacy during that same period. In addition, account should be taken of the period needed for the adoption of the measures necessary to comply with this judgment.
- 74 It is therefore appropriate to preserve the effect of the decision on adequacy until 30 September 2006, but its effect shall not be preserved beyond the date upon which the Agreement comes to an end.

**Costs**

- 75 Under Article 69(2) of the Rules of Procedure, the unsuccessful party is to be ordered to pay the costs if they have been applied for in the successful party's pleadings. Since the Parliament has applied for costs and the Council and the Commission have been unsuccessful, the Council and the Commission must be ordered to pay the costs. Pursuant to the first subparagraph of Article 69(4), the interveners in the present cases must bear their own costs.

On those grounds, the Court (Grand Chamber) hereby:

1. **Annuls Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection and Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection;**
2. **Preserves the effect of Decision 2004/535 until 30 September 2006, but not beyond the date upon which that Agreement comes to an end;**
3. **Orders the Council of the European Union to pay the costs in Case C-317/04;**
4. **Orders the Commission of the European Communities to pay the costs in Case C-318/04;**
5. **Orders the Commission of the European Communities to bear its own costs in Case C-317/04;**
6. **Orders the United Kingdom of Great Britain and Northern Ireland and the European Data Protection Supervisor to bear their own costs.**

[Signatures]

---

\* Language of the case: French.

□



Privacy Impact Assessment  
for the

# Automated Targeting System

November 22, 2006

**Contact Point**

**Phil Landfried**

**Office of Information and Technology**

**U.S. Customs and Border Protection**

**(703) 822-6237**

**Reviewing Official**

**Hugo Teufel III**

**Chief Privacy Officer**

**Department of Homeland Security**

**(571) 227-3813**



## Abstract

The Department of Homeland Security (DHS), Customs and Border Protection (CBP) has developed the Automated Targeting System (ATS). ATS is one of the most advanced targeting systems in the world. Using a common approach for data management, analysis, rules-based risk management, and user interfaces, ATS supports all CBP mission areas and the data and rules specific to those areas. This PIA is being conducted in conjunction with the System of Records Notice (SORN) that was published on November 2, 2006 in the *Federal Register*.

## Introduction

ATS is an Intranet-based enforcement and decision support tool that is the cornerstone for all CBP targeting efforts. CBP uses ATS to improve the collection, use, analysis, and dissemination of information that is gathered for the primary purpose of targeting, identifying, and preventing potential terrorists and terrorist weapons from entering the United States. Additionally, ATS is utilized by CBP to identify other violations of U.S. laws that are enforced by CBP. In this way, ATS allows CBP officers to focus their efforts on travelers and cargo shipments that most warrant greater scrutiny. ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data and personal information to form a more complete picture of a traveler, import, or export in context with previous behavior of the parties involved. Every traveler and all shipments are processed through ATS, and are subject to a real-time rule based evaluation.

ATS provides equitable treatment for all individuals in developing any individual's risk assessment score, because ATS uses the same risk assessment process for any individual using a defined targeting methodology for a given time period at any specific port of entry.

ATS receives various data in real time from the following different CBP mainframe systems: the Automated Commercial System (ACS), the Automated Export System (AES), the Automated Commercial Environment (ACE), and the Treasury Enforcement Communication System (TECS). ATS collects certain data directly from commercial carriers in the form of a Passenger Name Record (PNR). Lastly, ATS also collects data from foreign governments and certain express consignment services in conjunction with specific cooperative programs.

ATS accesses data from these sources, which collectively include electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers; land-border crossing and referral records for vehicles crossing the border; airline reservation data; nonimmigrant entry records; and records from secondary referrals, incident logs, suspect and violator indices, and seizures.

In addition to providing a risk-based assessment system, ATS provides a graphical user interface (GUI) for many of the underlying legacy systems from which ATS pulls information. This interface improves the user experience by providing the same functionality in a more rigidly controlled access environment than the underlying system. Access to this functionality of ATS uses existing technical security and privacy safeguards associated with the underlying systems.



ATS consists of six modules that provide selectivity and targeting capability to support CBP inspection and enforcement activities.

- ATS-Inbound – inbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Outbound – outbound cargo and conveyances (rail, truck, ship, and air)
- ATS-Passenger (ATS-P) – travelers and conveyances (air, ship, and rail)
- ATS-Land (ATS-L) - private vehicles arriving by land
- ATS - International (ATS-I) - cargo targeting for CBP's collaboration with foreign customs authorities
- ATS-Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)

Five of these modules are operational and subject to recurring systems' maintenance. They are: the ATS cargo modules, import, and export (ATS Inbound and ATS Outbound); the ATS-Passenger module; the ATS-Land module; and ATS-Analytical module. The ATS-International module is being developed to support collaborative efforts with foreign customs administrations.

As part of an ongoing effort to review and update system of records notices, CBP published a new SORN for ATS in the *Federal Register* on November 2, 2006 located at 71 FR 64543. This information collection was previously covered by the legacy TECS SORN.

### ATS System Overview

Currently, ATS consists of six modules that focus on exports, imports, passengers and crew (airline passengers and crew on international flights, passengers and crew on sea carriers), private vehicles crossing at land borders, and import trends over time. ATS assists CBP officers at the borders effectively and efficiently identify cargo, individuals, or conveyances that may present additional risk to the United States. A large number of rules are included in the ATS modules, which encapsulate sophisticated concepts of business activity that help identify suspicious or unusual behavior. The ATS rules are constantly evolving to both meet new threats and refine existing rules. ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. ATS is consistent in its evaluation of risk associated with individuals and is used to support the overall CBP law enforcement mission.

- *ATS-Inbound* is the primary decision support tool for inbound targeting of cargo. This system is available to CBP officers at all major ports (air/land/sea/rail) throughout the United States, and also assists CBP personnel in the Container Security Initiative (CSI) decision-making process. ATS Inbound provides CBP officers and Advance Targeting Units (ATU) with an efficient, accurate, and consistent method for targeting and selecting high-risk inbound cargo for intensive examinations. ATS-Inbound assists in identifying imported cargo shipments, which pose a high risk of containing weapons of mass effect, narcotics, or other contraband. ATS-Inbound increases the effectiveness of CBP officers dealing with imported cargo by improving the accuracy of the targeting of weapons of mass effect, narcotics or other contraband, commercial fraud violations, and other violations of U.S. law. The approach is to process data pertaining to entries and manifests



# Homeland Security

## Privacy Impact Assessment

Customs and Border Protection, Automated Targeting System

November 22, 2006

Page 4

against a variety of rules to make a rapid automated assessment of the risk of each import. Entry and manifest data is received from the Automated Manifest System (AMS), Automated Broker Interface (ABI), and the Automated Commercial Environment (ACE).

- *ATS-Outbound* is the outbound cargo targeting module of ATS that assists in identifying exports which pose a high risk of containing goods requiring specific export licenses, narcotics, or other contraband. *ATS-Outbound* uses Shippers' Export Declaration (SED) data that exporters file electronically with CBP's AES.<sup>1</sup> The SED data extracted from AES is sorted and compared to a set of rules and evaluated in a comprehensive fashion. This information assists CBP officers with targeting and/or identifying exports with potential aviation safety and security risks, such as hazardous materials and Federal Aviation Administration (FAA) violations. In addition, *ATS-Outbound* identifies the risk of specific exported cargo for such export violations as smuggled currency, illegal narcotics, stolen vehicles or other contraband.
- *ATS-Passenger* (*ATS-P*) is the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crewmembers prior to arrival or departure. It assists the CBP officer's decision-making process about whether a passenger or crewmember should receive additional screening prior to entry into or departure from the country because the traveler may pose a greater risk for violation of U.S. law. The system analyzes the Advance Passenger Information System (APIS) data from TECS, Passenger Name Record (PNR) data from the airlines, TECS crossing data, TECS seizure data, and watched entities. *ATS-P* processes available information from these databases to develop a risk assessment for each traveler. The risk assessment is based on a set of National- and user-defined rules which are comprised rule sets that pertain to specific operational/tactical objectives or local enforcement efforts.
- *ATS-Land* (*ATS-L*) is a module of ATS that provides for the analysis and rule-based risk assessment of private passenger vehicles crossing the nation's borders. By processing and checking of the license plate numbers of vehicles seeking to cross the border, *ATS-L* allows CBP officers to cross-reference the TECS crossing data, TECS seizure data, and State Department of Motor Vehicle (DMV) data<sup>2</sup> to employ the weighted rules-based assessment system of ATS. In this way *ATS-L* provides, within seconds, a risk assessment for each vehicle that assists CBP Officers at primary booths in determining whether to allow a vehicle to cross without further inspection or to send the vehicle for secondary evaluation.

---

<sup>1</sup> The Shipper's Export Declaration (SED), Commerce Form 7525-V, is used to compile the official U.S. export statistics for the United States and for export control purposes. The regulatory provisions for preparing, signing and filing the SED are contained in the Foreign Trade Statistics Regulations (FTSR), Title 15 Code of Federal Regulations (CFR) Part 30.

<sup>2</sup> DMV data to support *ATS-L* is obtained from a government source, National Law Enforcement Telecommunications System (NLETS). DMV data obtained to support *ATS-L* will only be used to support land border targeting applications. Access to the *ATS-L* application and the DMV data it uses are limited to DHS users including CBP officers and Border Patrol Agents. No other use or dissemination of DMV data will be performed by CBP.



- *ATS-International (ATS-I)* is being developed to provide foreign customs authorities with controlled access to automated cargo targeting capabilities and provide a systematic medium for exchanging best practices and developing and testing targeting concepts. The exchange of best practices and technological expertise can provide vital support to other countries in the development of effective targeting systems that can enhance the security of international supply chains and fulfill the objective of harmonizing targeting methodologies. If information from foreign authorities is run through the ATS-I module, it may also, consistent with applicable cooperative arrangements with that foreign authority, be retained in ATS-I by CBP to enhance CBP's targeting capabilities.
- *ATS-Trend Analysis and Analytical Selectivity (ATS-TAP,)* improves CBP's ability to examine, locate, and target for action violators of US laws, treaties, quotas, and policies regarding international trade. *ATS-Analytical* offers trend analysis and targeting components. The trend analysis function summarizes historical statistics that provide an overview of trade activity for commodities, importers, manufacturers, shippers, nations, and filers to assist in identifying anomalous trade activity in aggregate.

ATS supports the decision-making process and reinforces the role of the trained professionals making independent decisions necessary to identify violations of U.S. law at the border.

## Section 1.0 Information Collected and Maintained

The following questions are intended to define the scope of the information requested as well as the reasons for its collection as part of the system, rule, and/or technology being developed.

### 1.1 What information is to be collected?

Generally, ATS collects and maintains personally identifiable information relating to name, risk assessment, and the internal system rules upon which the assessment is based and Passenger Name Record data obtained from commercial carriers.

In order to build the risk assessment, ATS uses data obtained from other governmental information systems including: electronically filed bills, entries, and entry summaries for cargo imports; shippers' export declarations and transportation bookings and bills for cargo exports; manifests for arriving and departing passengers and crew; airline reservation data; nonimmigrant entry records; and records from secondary referrals, CBP incident logs, suspect and violator indices, state Department of Motor Vehicle Records, and seizure records.

- *ATS-Inbound:* Collects information about importers, cargo, and conveyances used to facilitate the importation of cargo into the United States. This includes personally identifiable information (e.g., name, address, birth date, government issued identifying records, where available and applicable) concerning individuals associated with imported cargo: brokers, carriers, shippers, buyers, sellers, and crew.



# Homeland Security

## Privacy Impact Assessment

Customs and Border Protection, Automated Targeting System

November 22, 2006

Page 6

- **ATS-Outbound:** Collects information about exporters, cargo, and conveyances used to facilitate the exportation of cargo from the United States. This includes personally identifiable information (e.g., name, address, birth date, government issued identifying records, where available and applicable) concerning individuals associated with exported cargo: brokers, carriers, shippers, buyers, sellers, and crew.
- **ATS-P:** Collects information about passengers and crew entering or departing the United States. This data includes passenger and crew manifests (through APIS), immigration control information, and PNR data. The PNR data may include such items as name, address, flight, seat number, and other information collected by the airline in connection with a particular reservation (Appendix B contains a list of PNR data elements). Not all carriers capture the same amount of information; the number of items captured may even vary among individual PNR from the same carrier.
- **ATS-L:** Collects information about vehicles and persons entering the U.S. at land border ports of entry. This data includes license plate numbers for vehicles entering the United States, vehicle, and registered owner data (derived from state DMV records). ATS-L receives license plate number via TECS. Using that license plate number, ATS-L then queries DMV data via National Law Enforcement Telecommunications System (NLETS) to obtain registration information for that vehicle (name, date of birth, address of the registered owner).
- **ATS-I:** Provides an interface for access to cargo targeting functionality by foreign customs authorities, as defined in separate information sharing arrangements. ATS-I permits foreign customs authorities to view restricted cargo information in ATS-Inbound coming from or to their nations, according to their own queries, or to add data, separately collected from their own systems, to be targeted against the developed screening queries. ATS-I collects trade data and related personally identifiable information (e.g., name, address, birth date, government issued identifying records, where available and applicable) collected by foreign customs authorities, in accordance with the applicable MOU negotiated for data sharing and access with that customs authority.
- **ATS-TAP:** Aggregates entry summary declarations to enable analysis of trends in trade activity and selective targeting of summary transactions related to identified anomalies.

ATS obtains information from the various sources identified in Appendix A. The information in these data files is cross-referenced between databases to correlate and augment information pertaining to an individual for purposes of screening or risk assessing. ATS permits user analysis of these risk assessments for purposes of targeting persons and commodities requiring further scrutiny or examination. As part of this risk assessing, ATS incorporates watched entities, including persons, data that is obtained from other government agencies and accessed through TECS.

## **1.2 From whom is information collected?**

ATS does not collect information directly from individuals. The information maintained in ATS is either collected from private entities providing data in accordance with U.S. legal requirements (e.g., PNR from air carriers regarding individual passengers) or is created by ATS as part of the risk assessment and associated rules.

The information used by ATS to build the risk assessment is collected from government data sources and from private entities providing data in accordance with U.S. legal requirements or other applicable arrangements (e.g. inward and outward manifests, merchandise entries).

## **1.3 Why is the information being collected?**

Personally identifiable information is collected to ensure that people and cargo entering or exiting the United States comply with all applicable U.S. laws. Relevant data, including personally identifiable information, is necessary for CBP to assess effectively and efficiently the risk and/or threat posed by a person, a conveyance operated by person, or cargo handled by a person, entering or exiting the country. CBP's ability to identify possible violations of U.S. law or other threats to national security would be critically impaired without access to this data. ATS permits all such information to be applied more efficiently and effectively to support both CBP's law enforcement mission, while also facilitating legitimate travel, trade, commerce, and immigration.

## **1.4 How is the information collected?**

The information that ATS uses is collected from government data sources (e.g., other government databases) and from entities providing data in accordance with U.S. legal requirements or other applicable arrangements (e.g., PNR from air carriers regarding individual passengers). ATS does not collect additional information directly from individuals.

Personally identifiable information that is collected through other government databases, such as TECS, ACE, ACS, AMS, APIS, AES, and National Crime Information Center (NCIC), is collected and stored in source systems of records. This information is collected by CBP in those systems to assist it in carrying out its law enforcement responsibilities relative to the importation or exportation of cargo, or the entry or exit of persons from the United States.

## **1.5 What specific legal authorities/arrangements/agreements define the collection of information?**

ATS-Outbound and ATS-Inbound supports CBP functions mandated by Title VII of Public Law 104-208, which provides funding for counter-terrorism and drug law enforcement. ATS-Outbound also supports functions arising from the Anti-Terrorism Act of 1997, the Clinger-Cohen Act, the Paperwork Reduction Act (PRA), and the Privacy Act. Both the PRA and the Privacy Act impose requirements and limits upon the government regarding the collection of information directly from persons, the flexibility of ATS's design and cross-referencing of databases permits CBP to employ information collected from persons, separately, for additional compatible uses



within a secure information system. The risk assessments for cargo that are conducted through ATS are also mandated under section 203 of the "Security and Accountability for Every Port Act of 2006" (SAFE Port Act) (P.L. 109-347) (October 11, 2006). ATS-P helps satisfy CBP's responsibilities arising from the Aviation and Transportation Security Act of 2001, which mandated the electronic transmission of APIS and PNR information to CBP; these requirements are vital to the protection of national security and were enacted as a result of the terrorist attacks of September 11, 2001, which revealed significant deficiencies in the area of aviation security. ATS-TAP was developed in response to analytical deficiencies identified in a Congressional GAO audit. ATS-TAP also addressed mandates to modernize import and export processing systems and to provide automated tools that assist in the administration and enforcement of international trade agreements. ATS-TAP gives CBP the capability to issue periodic compliance reports to Congress, set priorities for allocating available resources, and improves fiscal management associated with revenue collection.

## **1.6 Privacy Impact Analysis: Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.**

The privacy risks associated with the maintenance of the information in ATS include: the information may not be accurate or timely because it was not collected directly from the individual, the information could be used in a manner inconsistent with the privacy policy stated at the time of collection, and/or the individual may not be aware that the information is being used by ATS for the stated purposes and/or a negative CBP action could be taken in reliance upon computer generated information in ATS that has been skewed by inaccurate data.

To mitigate these privacy risks, CBP has done the following:

*Accurate and Timely Information.* The system generates a risk assessment; however, no action will be taken unless the information has been reviewed by a CBP officer trained in the interpretation of the information and familiar with the environment in which the information is collected and used. The ATS system supports CBP officers in identifying individuals or cargo that may pose a risk of violating U.S. laws or otherwise constitute a threat to national security, but it does not replace their discretion to determine whether the individual or cargo should be allowed into the country. If personally identifiable information is believed by the data subject to be inaccurate, a redress process has been developed and the individual is provided information about this process during the secondary review. See Section 7 of this PIA.

*Consistency with the stated privacy policy.* Prior to inclusion of information from system of records notices other than ATS, CBP reviews the routine uses and purposes statements to ensure that the purposes for which the information was collected and used are consistent with the law enforcement purposes of ATS. CBP officers are trained on the limited uses for which the information may be used in connection with their official duties.

*Lack of awareness of the use of information.* In order to increase transparency, CBP has published a SORN (see 71 FR 64543) and this PIA as means of informing individuals about the specific elements of ATS (ATS was previously considered a part of TECS). Additionally, before information

may be used in ATS the Privacy Act system of records notice must be reviewed by CBP to ensure the use is consistent with the stated purposes.

*Automatic negative determination.* As part of CBP's inspection policies and procedures no adverse action is taken by CBP with respect to an individual, cargo or conveyance until the relevant information is reviewed by a well-trained CBP officer.

## **Section 2.0 Uses of the System and the Information**

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

### **2.1 Describe all the uses of information.**

Authorized CBP officers and other government personnel located at seaports, airports, and land border ports around the world use ATS to support targeting, inspection, and enforcement related requirements.

ATS is a critical tool that enables CBP to improve the collection, use, analysis, and dissemination of intelligence to target, identify, and prevent potential terrorists and terrorist weapons from entering the United States and identify other violations and violators of U.S. law. The automated nature of ATS greatly increases the efficiency and effectiveness of the officer's otherwise manual and labor-intensive work, and thereby helps facilitates the more efficient movement of legitimate cargo and people while safeguarding the border and the security of the United States. In this way ATS facilitates international trade and travel while enhancing homeland and border security.

### **2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern?**

Yes. ATS builds a risk-based assessment for persons, cargo and conveyances based on criteria and rules developed by CBP. ATS maintains the risk assessment together with a record of which rules were used to develop the risk assessment.

The ATS rules and resulting risk assessments are designed to signal to CBP officers that further inspection of a person, shipment or conveyance may be warranted, even though an individual may not have been previously associated with a law enforcement action or otherwise be noted as a person of concern to law enforcement.

### **2.3 How will the information collected from individuals or derived from the system be checked for accuracy?**

ATS relies upon the source systems to ensure that data used by ATS is accurate and complete. Discrepancies may be identified in the context of a CBP officer's review of the data and the CBP officer will take action to correct that information, when appropriate. Although ATS is

not the system of record for most of the source data, ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real-time or near real-time from TECS, ACE, AMS, APIS, ACS, AES, and NCIC. When corrections are made to data in source systems, ATS updates this information immediately and only the latest data is used. In this way, ATS integrates all updated data (including accuracy updates) in as close to real-time as possible.

Furthermore, in the event personally identifiable information (such as PNR) used by and/or maintained in ATS is believed by the data subject to be inaccurate a redress process has been developed and the individual is provided information about this process during the secondary review. See Section 7 of this PIA.

To the extent information that is obtained from another government source (for example, DMV data that is obtained through NLETS) is determined to be inaccurate, this problem would be communicated to the appropriate government source for remedial action.

## **2.4 Privacy Impact Analysis: Given the amount and type of information collected, describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses.**

The privacy risks associated with the use of the information maintained in ATS include: additional inspection and misuse of data by users.

*Additional Inspection.* One risk to individuals from the use of ATS is to be referred to secondary inspection. Individuals are subject to random secondary inspection under U.S. law, so, all individuals are always at risk of referral to secondary inspection. Accordingly, the greatest impact that ATS can have on an individual is comparable to that of random inspection, a required component of the inspection process. As a decision support system, ATS operates according to the rules within the system that were created to parallel the policies and procedures that govern the CBP inspection process to ultimately protect individual's privacy rights. To the extent that an individual may be referred to secondary inspection based, in part, upon an analysis of information derived through ATS, this PIA and the SORN for ATS as well as the PIAs and SORNs for the source systems, from which ATS draws information, provide the greatest mitigation to the risk that information may be improperly obtained or inappropriately accessed or used.

ATS offers equitable risk assessment using a secure encrypted network; however, it is the policies and procedures and laws that govern the inspection process that ultimately protect individual privacy rights. The professionalism applied by CBP officers serves to further protect individual privacy rights.

*Misuse or Breach of ATS.* ATS User roles are highly restricted and audited. ATS has role-based access. Access is restricted in the form of Mandatory Access Control, which is based on a demonstrated "need to know." Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. CBP officers with access to ATS are required to

complete security and data privacy training on a biennial basis and their usage of the system is audited to ensure compliance with all privacy and data security requirements.

## **Section 3.0 Retention**

### **3.1 What is the retention period for the data in the system?**

The retention period for data in ATS reflects the underlying retention period for the data in its source records (for example, since the data from ACS, AMS, and ACE is retained for six years, the associated information in ATS is only retained for that period of time). Provided the data is not associated with an open investigation (in which it is retained until the investigation is closed), this retention period will not exceed forty years for the source record data and is forty years for the risk assessment and associated rules upon which the assessment is based

Generally, data maintained specifically by ATS will be retained for up to forty years. Certain data maintained in ATS may be subject to other retention limitations pursuant to applicable arrangements (e.g., PNR information derived from flights between the U.S. and the European Union). Cost and performance impact of data retention may lead to retention periods less than forty years.

### **3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?**

A NARA Electronic Records Appraisal Questionnaire was completed for Passenger Name Record (PNR) Data in spring 2005. Efforts are underway and ongoing to obtain NARA approval for the remaining data retained in ATS.

### **3.3 Privacy Impact Analysis: Given the purpose of retaining the information, explain why the information is needed for the indicated period.**

ATS maintains the risk assessment together with a record of which rules were used to develop the risk assessment. This assessment and related rules history associated with developing a risk-based assessment are maintained for up to forty years to support ongoing targeting requirements. Forty years of data retention as an outside limit is consistent with the longest retention period for the source records which constitute information maintained in ATS.

Nonetheless, The touchstone for data retention is the data's relevance and utility. Accordingly, CBP will regularly review the data maintained in ATS to ensure its continued relevance and usefulness. If no longer relevant and useful, CBP will delete the information.

All risk assessments need to be maintained because the risk assessment for individuals who are deemed low risk will be relevant if their risk attributes change in the future, for example, if new terrorist associations are identified. Additionally, certain data collected directly by ATS may be subject to shorter retention limitations pursuant to separate arrangements. The adoption of



shorter retention periods may not be publicly disclosed if DHS concludes that disclosure would affect operational security, for example by giving terrorism suspects the certainty that their past travel patterns would no longer be available to U.S. authorities.

## Section 4.0 Internal Sharing and Disclosure

### 4.1 With which internal organizations is the information shared?

The principal users of ATS data are within the Department of Homeland Security including:

- CBP Office of Field Operations (OFO)
- CBP Office of Intelligence (OI)
- CBP National Targeting Center (NTC)
- CBP Office of International Trade (OT)
- U.S. Immigration and Customs Enforcement (ICE)

The information collected through ATS may be shared with component agencies within DHS on a need to know basis consistent with the component's mission. Access to ATS is role-based according to the mission of the component and the user's need to know.

### 4.2 For each organization, what information is shared and for what purpose?

Authorized users from CBP OFO, OI, and the NTC have full access to all the ATS modules for purposes of enforcing U.S. laws related to the entry into and exit from the United States of persons, cargo, and conveyances. Authorized users from ICE and the DHS Office of the Secretary have been provided access to ATS-P, for purposes of carrying out their law enforcement and counter-terrorism responsibilities. Finally, data collected and/or maintained in ATS (including PNR) may be shared with any DHS component consistent with U.S. law, DHS and CBP policy, the ATS SORN, and any applicable arrangements or agreements.

### 4.3 How is the information transmitted or disclosed?

Data may be retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access the ATS web-based interface. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data maintained in ATS may also be shared with other components with a need to know on a case-by-case basis, consistent with U.S. law, DHS and CBP and DHS policies, and any applicable arrangements or agreements.



#### **4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.**

The key privacy risk concerns the potential number of DHS personnel with access to the system. This risk is mitigated and managed by employing user profiles that define rights and responsibilities concerning a user's access to data contained in the system. The principal method for determining what access rights and system responsibilities a user will have is reference to the user's need-to-know. Need-to-know determinations are covered by internal CBP policies and procedures that relate a user's mission or operational responsibilities to the specific sub-set of data, contained within ATS, that supports those functions. For example, users at a seaport on the East coast do not have access to current risk assessment data associated with an arriving air traveler at a West coast airport. ATS retains audit logs for all user access, these logs are reviewed to ensure that a user should have no more access than is minimally necessary to perform his or her job. Lastly, users are subject to periodic renewal of their access and regular privacy awareness training to maintain attentiveness to the need for safeguarding and the liabilities for inappropriate use or sharing of ATS protected information.

## **Section 5.0 External Sharing and Disclosure**

### **5.1 With which external organizations is the information shared?**

For the information maintained in ATS (name, risk assessment, rules applied, and PNR), a limited number of users outside of DHS have access to this information. Only if there is a specific information sharing arrangement permitting the development of an outside agency specific rule sub-set will users from that outside agency be permitted to access and review the name, risk assessment, and rules fired based on the rules developed for the outside agency.

Currently such information sharing agreements exist with the following:

- ATS-Inbound access outside of DHS, for access to information regarding imported commodities, include:
  - U.S. Department of Agriculture (this access includes viewing of specific USDA risk assessments and rule sets)
  - U.S. Food and Drug Administration (FDA) (limited to personnel at the FDA Prior Notice Center)
  - Canada Border Security Agency (CBSA) (See section 5.2 below)
- ATS-Outbound access outside of DHS, for access to information regarding exported commodities, include:
  - U.S. Department of Commerce Bureau of Industry and Security



- The Mexican government, through a Memorandum of Understanding (MOU), may submit queries to CBP seeking verification of Mexican import data by U.S. export data. CBP uses ATS to perform the verification. The verification consists of a yes or no indicator regarding whether or not the two data sets are comparable, that is within or outside of a defined range of standard deviation pertaining to the reported value of the subject commodity. There is no direct access to ATS by Mexico, nor is there any transfer of personally identifiable information or specific trade data pursuant to this arrangement.
- ATS-P access outside of DHS:
  - Various law enforcement task forces outside of DHS require queries to be run against ATS-P data (for example, the FBI-led Joint Terrorism Task Force). Generally, these task force groups do not have direct access to ATS-P and must present a request for a query to the CBP representative that supports or is part of the requesting task force.
  - Access to PNR may also be facilitated for various law enforcement and counterterrorism agencies, through the receipt of direct requests and authorized releases.

As a graphical user interface for underlying older existing systems, users outside of DHS use ATS as an easier means of accessing these older existing systems. User access is tightly controlled and users may only access the source data consistent with their user roles in the underlying systems. In some instances users have less access through ATS than if they had direct access to the underlying system. Agencies with this type of access include:

- Department of Justice (Federal Bureau of Investigation)
- Department of State (Diplomatic Security)

## 5.2 What information is shared and for what purpose?

Data obtained from other systems (e.g., ACE, AES, TECS, and NCIC) is used to identify cargo conveyances and travelers at high risk for involvement in terrorist activities or for other statutory violations, such as drug smuggling, counterfeiting, and intellectual property rights infringement.

USDA users are supported by rule sets specific to the USDA for enforcement of compliance with meat and poultry inspection regulations and other perishable commodity restrictions. USDA users can view the risk assessment and rule history for the USDA specific rule sets only. For all other rule sets, USDA users can view the source data, but may not view the risk assessment.

For all other ATS users outside of CBP, users may view the source data, but may not view the risk assessment. Access to ATS modules and underlying data, as previously stated, is determined by user profiles assigning a particular user rights and responsibilities dependent upon his or her operational and mission functions and authority.

Access to ATS-L and the DMV data for U.S. plated vehicles that it uses is limited to CBP Officers. No other use or dissemination of DMV data is performed.

Canada is currently the only foreign country that accesses data directly using ATS. CBSA users can only view Canadian data provided by Canada. Other countries may, through ATS-I, be permitted to use ATS, but they will likewise be limited to viewing their own data and the related risk assessment and rules applied, if expressly stated within the terms of their particular arrangement.

### **5.3 How is the information transmitted or disclosed?**

For facilitated disclosure, various users outside of DHS must present a request for a query to the CBP representative that supports or is part of the requesting user, task force, agency, etc. Upon CBP approval of the specific request for access, access may be provided either electronically or by hard copy print out.

ATS users access data using the ATS user interface. Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data is retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access to ATS web-based interface.

Access for users outside of DHS is limited to source data only (the access employs ATS as an interface to the ATS image of the underlying database).

### **5.4 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared through the system, and does the agreement reflect the scope of the information currently shared?**

Yes, there are agreements in place to share information from ATS. Each agreement defines the nature of access to ATS, including specific modules and scope of information subject to the sharing arrangement. In defining the sharing arrangement, the agreements also set forth the terms and conditions of access to information and the limitations upon the use and redissemination of the information. As an example and as previously noted, the Mexican government is an indirect beneficiary of ATS-Outbound data and is permitted to submit a request for a query to CBP in accordance with an agreement (Memorandum of Understanding, MOU<sup>3</sup>) between CBP and the Mexican government. If CBP approves the request for query is approved, a response is forwarded using secure electronic messaging. (See section 5.1 above.)

---

<sup>3</sup> CBP has the authority to provide information to foreign customs and law enforcement agencies pursuant to Title 19, United States Code, Section 1628, and more specifically with respect to the CGA, as provided for under to the Agreement between the Government of the United States of America and the Government of the United Mexican States Regarding Mutual Assistance Between their Customs Administrations (CMAA), dated June 20, 2000. This MOU is subject to the implementing guidelines contained within the CMAA.

## **5.5 How is the shared information secured by the recipient?**

The terms and conditions within agreements permitting access to ATS set forth the requirements that external users of ATS must meet in order to obtain and maintain access. Generally, CBP's requirements for external users require that the external user employ the same or similar security and safeguarding precautions as employed by CBP. For CBP, ATS has role-based security. Users from other government organizations must use the ATS interface to access the system where access is limited via a user profile/role. ATS User roles are highly restricted and audited. Application access is restricted in the form of Mandatory Access Control, which is based on a demonstrated "need to know."

## **5.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?**

CBP requires all external users of ATS information to receive the same training as CBP users regarding the safeguarding, security, and privacy concerns relating to information stored in the ATS database. This means that users are subject to periodic recertification of their access (typically every six months), that they receive initial functional training related to their particular access and role, and that they are required to complete and pass a system based privacy awareness course (initially before access, and every two years, thereafter).

## **5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.**

When sharing information with external agencies, similar risks are posed as those arising with respect to internal sharing with DHS. To this extent the agreements with external agencies require similar measures to be employed relating to security, privacy, and safeguarding of information. Separately, an additional risk is posed by the potential for further dissemination of information by the external agency to a third agency. Again, the terms and conditions of the agreement, which provides for access by an external agency, address and mitigate this risk, in the confidentiality section of each agreement, by requiring any further dissemination of shared data outside of the receiving agency to be subject to prior authorization by CBP. Lastly, CBP emphasizes that, within each agreement, each external user is provided with training, as outlined in paragraph 5.6, designed to ensure that data that is accessed through ATS is safeguarded and secured in an appropriate manner, consistent with applicable laws and policies.

## **Section 6.0 Notice**

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.



## **6.1 Was notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?**

ATS does not collect any information directly from individuals. ATS does collect and maintain passenger name record (PNR) data derived from air carrier reservation/departure control systems, as indicated in the SORN for ATS published on November 2, 2006 at 71 FR 64543 and discussed above at paragraph 1.1.

In cases where an individual has a concern about the information collected during an interaction with a CBP officer, the CBP officer may provide the individual with a copy of the IBIS Fact Sheet (See Appendix), which provides both general information concerning CBP's border enforcement mission and responsibilities, and specific information concerning where to direct inquiries about CBP's actions or the information collected.

Most of the information that ATS uses is collected from government data sources. Notice was provided for under the applicable source systems of records and privacy impact assessments (where applicable), as well as through the publication of the laws and regulations authorizing the collection of such information. This information is collected and stored in the source systems of record, is collected for other purposes, and would be collected with or without ATS.

This information is collected by CBP primarily for law enforcement purposes related to the entry and exit of people, cargo, and conveyances; use of this data also facilitates legitimate trade and immigration.

## **6.2 Do individuals have an opportunity and/or right to decline to provide information?**

Generally, the decision whether to travel to or import goods/merchandise into a foreign country is within the discretion of the individual. United States law requires individuals seeking to enter the country to identify themselves and demonstrate admissibility to the United States; likewise, persons seeking to import goods and merchandise in the U.S. are required to provide certain information to allow CBP to determine whether the goods/merchandise may enter the U.S. ATS does not require individuals to provide information beyond that authorized by law. This information is captured by the source systems (e.g., ATS, ACS, and TECS) and used by ATS to efficiently and expeditiously identify persons, conveyances, and cargo that may pose a concern to law enforcement, resulting in further review by appropriate government officers.

While ATS does not collect information directly from individuals, it employs information obtained from persons by these source systems. The only way an individual can decline to provide information is to refrain from traveling to, through, or over the United States or by not bringing in, shipping, or mailing any goods/merchandise to the United States.



### **6.3 Do individuals have the right to consent to particular uses of the information, and if so, how does the individual exercise the right?**

Any consent individuals may grant is controlled by the source systems described in earlier sections.

Because the submission of information is required in order to travel to, through, or over the United States or to bring in, ship, or mail any goods/merchandise to the United States restrictions on CBP use and sharing of accessed information are limited to legal requirements set forth in the Privacy Act, Trade Secrets Act, and the uses published in System of Records Notices (SORN). Consent to store or use this information must be done in accordance with the above legal requirements.

ATS does not directly collect information from individuals. Opportunities for individuals to consent to particular uses of information would be addressed using the process defined by the source systems. As all information collected by these systems is mandated by law, there is effectively no consent mechanism other than the choice not to travel or ship items.

Many air carriers have provided their own notice to customers concerning these requirements.

### **6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.**

There is a risk that the individual may not know that the information is being used by ATS in the ways described. As such, CBP has published the System of Records Notice and this PIA to increase transparency of its operations. Additionally, it has drafted language for commercial carriers to include in their privacy statements so as to provide further transparency.

## **Section 7.0 Individual Access, Redress and Correction**

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

### **7.1 What are the procedures which allow individuals to gain access to their own information?**

Procedures for individuals to gain access to data maintained in source systems that provide data used by ATS would be covered by the respective SORNs for the source systems. In addition, the Freedom of Information Act (FOIA) (5 U.S.C. 552) provides a means of access to information, including PNR data, for all persons, irrespective of the individual's status under the Privacy Act.

With respect to data for which ATS is the actual source system (e.g., PNR), the applicable SORN is published at Volume 71, Federal Register 64543 (November 2, 2006). FOIA requests for

access to information for which ATS is the source system may be directed to CBP in the manner prescribed by regulations at Title 19, Code of Federal Regulations, Part 103.

With respect to the data that ATS creates, i.e., the risk assessment for an individual, the risk assessment is for official law enforcement use only and is not communicated outside of CBP staff, nor is it subject to access under the Privacy Act. ATS is a system that supports CBP law enforcement activities, as such an individual might not be aware of the reason additional scrutiny is taking place, nor should he or she as this may compromise the means and methods of how CBP came to require further scrutiny. Additional screening may occur because of a heightened risk assessment, or because of other concerns by the CBP officer, or on a random basis. If a reviewing officer determines that a person is not a match to a record or the record is determined to not be accurate, CBP has a policy in place which permits the officer to promptly initiate corrective action with regard to that record to avoid that person being identified for examination during future entry or exit processing based on that erroneous information.

## **7.2 What are the procedures for correcting erroneous information?**

CBP has created a Customer Satisfaction Unit in its Office of Field Operations to provide redress with respect to inaccurate information collected or maintained by its electronic systems, which include ATS, TECS, IBIS, and APIS). Inquiries to the Customer Satisfaction Unit should be addressed to: Customer Satisfaction Unit, Office of Field Operations, U.S. Customs and Border Protection, Room 5.5C, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Individuals making inquiries should provide sufficient information to identify the record at issue.

DMV data to support ATS-L is obtained from a government source, NLETS. If problems with the DMV data are identified through the redress process, the problem would be communicated to NLETS. Upon request, CBP officers will provide the IBIS fact sheet that provides information on appropriate redress. The redress process includes the ability to correct data in the source systems including TECS and IBIS.

ATS incorporates the procedures of the source systems with respect to error correction. Once any updates or corrections are made, they are transmitted to ATS. Corrected data becomes available to ATS almost immediately after the correction is entered to the source system. ATS monitors source systems for changes to the source system databases. Continuous source system updates occur in real-time, from ACS, AES, and TECS. When corrections are made to data in source systems, ATS reflects these updates to data, accordingly.

## **7.3 How are individuals notified of the procedures for correcting their information?**

Upon request, CBP officers will provide the IBIS fact sheet that provides information on appropriate redress. The redress procedure provides the ability to correct data in the source systems include TECS and IBIS. Publication of the source system SORNs also provides information on accessing and amending information collected through those systems. There is no procedure to correct the risk assessment and associated rules stored in ATS as the assessment is based on the underlying data and will change when the data from source system(s) is amended.



## **7.4 If no redress is provided, are alternatives available?**

Redress is provided.

## **7.5 Privacy Impact Analysis: Given the access and other procedural rights provided for in the Privacy Act of 1974, explain the procedural rights that are provided and, if access, correction and redress rights are not provided please explain why not.**

As set forth in the ATS SORN (71 FR 64543, November 2, 2006), pursuant to 31 CFR § 1.36 pertaining to the Treasury Enforcement Communications System, ATS, which was previously covered by the Treasury Enforcement Communications System (TECS) system of records notice and associated with the below exemptions, records and information in this system are exempt from a number of provisions of the Privacy Act (5 U.S.C. 552a (c)(3), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(4)(G), (H), and (I), and (f) ) pursuant to 5 U.S.C. 552a (j)(2) and (k)(2)). DHS intends to review these exemptions and, if warranted, issue a new set of exemptions specific to ATS within ninety (90) days of the publication of this notice. However, as noted above in paragraph 7.1, individuals may seek access to information collected in ATS or originating from a government source system pursuant to the FOIA, and as a matter of CBP policy, redress may also be requested in the manner described above in paragraph 7.2.

## **Section 8.0 Technical Access and Security**

The following questions are intended to describe technical safeguards and security measures.

### **8.1 Which user group(s) will have access to the system?**

All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and responsibilities of each user. Access by Users, Managers, System Administrators, Developers, and others to the ATS data is defined in the same manner and employs profiles to tailor access to mission or operational functions. User access to data is based on a demonstrated need-to-know basis.

### **8.2 Will contractors to DHS have access to the system?**

Yes, subject to the same background, training, need-to-know, and confidentiality requirements as employees.

### **8.3 Does the system use “roles” to assign privileges to users of the system?**

Yes, ATS user access is restricted in the form of Mandatory Access Controls assigned based on the user’s role. Users cannot assign their roles to any other user, nor can they elevate their own rights within the system. User access is enforced with the ATS Security Desk procedures referenced in the section above and roles are assigned only after supervisor request, process owner approval, and appropriate security checks have been confirmed.

### **8.4 What procedures are in place to determine which users may access the system and are they documented?**

Initial requests for grants to the system are routed from the user through their supervisor to the specific CBP Process Owners. Need-to-know determinations are made at both the supervisor and process owner level. If validated, the request is passed on to the Security Help Desk. Once received, System Security Personnel are tasked to determine the user Background Investigation (BI) status. Once the BI is validated, the user’s new profile changes are implemented. The user, supervisor and Process Owner are notified via email that the request has been processed along with instructions for the initial login. These records are maintained by CBP. Profile modification requests follow the same process as for an initial request. If an individual has not used the system for more than 90 days, that individual’s access will be denied and the same procedures as noted above must be completed to renew access. In addition, on a periodic basis access is reviewed by the process owner, on a periodic basis, to ensure that only appropriate individuals have access to the system.

### **8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?**

ATS User roles are highly restricted and audited.

Application access is restricted in the form of Mandatory Access Control, which is based on a demonstrated “need to know.” Data may only be accessed using the CBP network with encrypted passwords and user sign-on functionality. Data is retrieved through authorized users logging in to the CBP network remotely using encryption and passwords to access to ATS web-based interface.

### **8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?**

On a periodic basis access is reviewed by the process owner to ensure that only appropriate individuals have access to the system. Additionally, CBP’s Office of Internal Affairs conducts periodic reviews of the ATS system in order to ensure that the system is being accessed and used in accordance with documented DHS and CBP policies.



## **8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?**

The CBP process owners and all system users are required to complete bi-annual training in privacy awareness. If an individual does not take training, he/she will lose access to all computer systems, which are integral to his/her duties as a CBP Officer.

## **8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?**

ATS underwent the Certification and Accreditation (C&A) process in accordance with Customs and Border Protection policy, which complies with these Federal statutes, policies, and guidelines, and was certified and accredited on June 16, 2005, for a three year period.

A Security Risk Assessment was completed on March 28, 2006 in compliance with FISMA, OMB policy and NIST guidance.

## **8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.**

Privacy risks identified with respect to access and security were in appropriate use and access of the information. These risks are mitigated through training, background investigations, internal system audit controls, CBP Code of Conduct and Disciplinary system, and the practice of least privileged access.

## **Section 9.0 Technology**

### **9.1 Was the system built from the ground up or purchased and installed?**

ATS was built from the ground up.

The data collected through ATS is maintained using existing data models in the source systems of records.

### **9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.**

Integrity, privacy, and security are analyzed as part of the decisions made for ATS in accordance with CBP security and privacy policy from the inception of ATS, as demonstrated by the successful transition through the systems development lifecycle (SDLC), certification and

accreditation, and investment management processes. Particular areas that were identified as needing to be addressed during the development included: use of accurate data, system access controls, and audit capabilities to ensure appropriate use of the system.

### **9.3 What design choices were made to enhance privacy?**

The system was developed so that the rules are building risk assessments based on the most accurate information available in the source systems. This improves the data integrity of the system. User access controls were developed in order to ensure that only the minimum number of individuals with a need to know the information are provided access to the information. Audit provisions in conjunction with policies and procedures were also put in place to ensure that the system is properly used by CBP officers.

The system is designed to provide the following privacy protections:

- Equitable risk assessment:
  - ATS provides equitable treatment for all individuals. Equitable risk assessment is provided because ATS uses the same risk assessment process for everybody (using a defined targeting methodology for a given period at a specific port).
  - ATS applies the same methodology to all individuals to preclude any possibility of disparate treatment of individuals or groups. ATS is consistent in its evaluation of risk associated with individuals and is used to support the overall CBP law enforcement mission.
  - ATS supports a national targeting policy that is established at the National Targeting Center. CBP policies regarding inspections and responding to potential terrorists and other criminals seeking entry into the United States are documented in various CBP Directives and individuals with access to the system are trained on the appropriate use of the information.
- CBP's secure encrypted network:
  - ATS security processes, procedures, and infrastructure provide protection of data, including data about individuals that is stored in ATS databases.
  - Encryption and authentication are the technical tools used to protect all ATS data, including data about individuals.
- ATS's role as a decision support tool for CBP officers:
  - As a decision support system, ATS is employed to support but not replace the decision-making responsibility of CBP officers and analysts. The information accessed in ATS is not the conclusion about whether or not to act but merely part of the basis upon which a CBP officer will make his or her decision. Human



intervention, professionalism, and training all serve to mitigate the potential privacy threat posed by data comparisons made outside of an operational context. .

In order to enhance privacy and transparency, a separate and distinct System of Records under the Privacy Act was published to address both the risk assessments derived using ATS, the rules applied, as well as other information for which ATS is considered the actual source system (i.e, PNR). The SORN for ATS is published in Volume 71, Federal Register 64543 (November 2, 2006).

Additionally, access to the assessment and related rules is limited to a small number of CBP officers who have gone through extensive training on the appropriate use of the information and CBP targeting policies. These CBP officers are trained to review the risk assessments and the underlying information to identify cargo and individuals that truly pose a risk to law enforcement.

## Conclusion

ATS is a decision support tool used by CBP officers to identify individuals, cargo and conveyances that may require additional scrutiny based on observations related to data describing those individuals.

The ATS system supports CBP officers in identifying individuals or cargo that may be a risk to U.S. law enforcement, but it does not replace their judgment in determining whether the individual or goods/merchandise, as applicable, should be allowed into the country.

ATS offers equitable risk assessment using a secure encrypted network; however, it is the policies and procedures and laws that govern the inspection and other law enforcement processes that ultimately protect individual privacy rights. The professionalism applied by CBP officers serves to further protect individual privacy rights.



## **Appendix A: Detailed Description of Information Sources Being Compiled**

The information ATS uses is described by module and is presented in the following format.

- Nature, Source

*ATS- Inbound:* Collects information about Importers and cargo and conveyances used to import cargo to the United States from destinations outside its borders. Information regarding individuals, such as importers, that is collected in connection with items identified below, include, but are not limited to,

- Sea/Rail Manifests (bills of ladings), Automated Manifest System (AMS)
- Cargo Selectivity Entries, Automated Broker Interface (ABI)
- Entry Summary Entries, ABI
- Air Manifest (bills of lading), AMS-Air
- Express Consignment Services (bills of lading)
- CCRA Manifest (bills of ladings), Canada Customs and Revenue (CCRA)
- CAFÉ, QP Manifest Inbound (bills of ladings), AMS
- Truck Manifest, Automated Commercial Environment (ACE)
- Inbound Data (bills of ladings), AMS
- Food and Drug Administration (FDA) Entries/Prior Notice (PN), Automated Commercial System (ACS)
- Census Import Data, Department of Commerce

*ATS-Outbound:* Collects information about exporters and cargo and conveyances used to transport cargo from the United States to destinations outside its borders.

- Shippers Export Declarations, Automated Export System (AES)
- Export Manifest Data, AES
- Export Air Way Bills of Lading
- Census Export Data, Department of Commerce



# Homeland Security

## Privacy Impact Assessment

Customs and Border Protection, Automated Targeting System

November 22, 2006

Page 26

ATS-L: Collects information about vehicles and persons crossing land border locations. This data includes license plate numbers for vehicles entering the United States, vehicle and registered owner data (derived from state DMV records).

- Publicly Available State DMV Data
- Border Crossing, TECS
- Seizures, TECS

ATS-P: Collects information about travellers entering the United States from destinations outside its borders. This data includes passenger manifests, immigration control information and Passenger Name Record (PNR) information (for which ATS is the source system).

- Advance Passenger Information System (APIS)
- Border Crossing, TECS
- Land Border Crossing, TECS
- I94, TECS<sup>4</sup>
- Personal Search, TECS
- Secondary Referrals, TECS
- Secondary Referrals/Land, TECS
- Secondary Referrals/CBP/ICE, TECS
- Seized Property, TECS
- Seized Vehicle, TECS
- USVISIT, TECS<sup>5</sup>
- NCIC III, TECS
- Air Craft Arrivals, ACS
- PNR (Approximately 100 airlines), Airline Reservations System data collected in ATS
- Visa, TECS
- Enforcement Subjects: Person, TECS
- Enforcement Subjects: Business, TECS
- Enforcement Subjects: Address, TECS

<sup>4</sup> ATS receives I94 data via TECS. TECS receives I94 data directly from the source ICE system.

<sup>5</sup> ATS receives USVISIT data via TECS. TECS receives US VISIT data directly from USVISIT.



# Homeland Security

## Privacy Impact Assessment

Customs and Border Protection, Automated Targeting System

November 22, 2006

Page 27

ATS-TAP: Collates information derived from ATS- Outbound and ATS-Inbound.

ATS also uses watched entities data:

- Debarred Parties, Dept of State ODTIC
- Nuclear Proliferation, Dept of Commerce BXA
- Specially Designated Parties, Dept of Treasury OFAC



## Appendix B PNR Data Elements

### PNR Data Elements May Include\*

1. PNR record locator code
2. Date of reservation
3. Date(s) of intended travel
4. Name
5. Other names on PNR
6. Number of travelers on PNR
7. Seat information
8. Address
9. All forms of payment information
10. Billing address
11. Contact telephone numbers
12. All travel itinerary for specific PNR
13. Frequent flyer information (limited to miles flown and address(es))
14. Travel agency
15. Travel agent
16. Code share PNR information
17. Travel status of passenger
18. Split/Divided PNR information
19. Identifiers for free tickets
20. One-way tickets
21. Email address
22. Ticketing field information
23. ATFQ fields
24. General remarks
25. Ticket number
26. Seat number
27. Date of ticket issuance
28. Any collected APIS information
29. No show history
30. Number of bags
31. Bag tag numbers
32. Go show information
33. Number of bags on each segment
34. OSI information
35. SSI information
36. SSR information
37. Voluntary/involuntary upgrades
38. Received from information
39. All historical changes to the PNR

\*Not all carriers collect PNR and of those that do collect this data, not all collect the same sets of PNR data.



## Appendix C IBIS Fact Sheet

# ***IBIS FACT SHEET***

### *What is IBIS?*

IBIS is the acronym for the Interagency Border Inspection System.

### *Who uses IBIS?*

In addition to U.S. Customs and Border Protection (CBP), law enforcement and regulatory personnel from 20 other federal agencies or bureaus use IBIS. Some of these agencies are the FBI, Interpol, DEA, ATF, the IRS, the Coast Guard, the FAA, Secret Service and the Animal Plant Health Inspection Service, just to name a few. Also, information from IBIS is shared with the Department of State for use by Consular Officers at U.S. Embassies and Consulates.

### *What does IBIS Provide?*

IBIS assists the majority of the traveling public with the expeditious clearance at ports of entry while allowing the border enforcement agencies to focus their limited resources on those potential non-compliant travelers. IBIS provides the law enforcement community with access to computer-based enforcement files of common interest. It also provides access to the FBI's National Crime Information Center (NCIC) and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems (NLETS).

### *Where is IBIS?*

IBIS resides on the Treasury Enforcement Communications System (TECS) at the CBP Data Center. Field level access is provided by an IBIS network with more than 24,000 computer terminals. These terminals are located at air, land, and sea ports of entry.

### *What information is in IBIS?*

IBIS keeps track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. IBIS terminals can also be used to access NCIC records on wanted persons, stolen vehicles, vessels or firearms, license information, criminal histories, and previous Federal inspections. The information is used to assist law enforcement and regulatory personnel.

### *Customs and Border Protection's collection of passenger name record information.*

U.S. Customs and Border Protection has the authority to collect passenger name record information on all travelers entering or leaving the United States. This information is strictly used for preventing and combating terrorism and serious criminal offenses, with the principal purpose of facilitating U.S. Customs and Border Protection's mission to protect the borders through threat analysis to identify and interdict persons who have committed or may potentially commit a terrorist act.

### *Additional Questions?*

Any concerns you may have as an international traveler or importer about the use or application of IBIS may be addressed to:

**U.S. Customs and Border Protection  
Freedom of Information Act/  
Customer Satisfaction Unit  
Room 5.5 C  
1300 Pennsylvania Avenue, N.W.  
Washington, D.C. 20229**

Please ensure that you provide a sufficient amount of personal identifying information (**legible** copy of your passport, driver's license, etc.) for CBP to perform an in-depth inquiry into your concerns.



**Homeland  
Security**

**Privacy Impact Assessment**

Customs and Border Protection, Automated Targeting System

November 22, 2006

Page 30

## **Responsible Officials**

Laurence Castelli, Chief, Privacy Act Policy and Procedures Branch, Office of Regulations and Rulings, CBP, (202) 572-8712.

## **Approval Signature Page**

---

Hugo Teufel III  
Chief Privacy Officer  
Department of Homeland Security

**Exhibit 4**

***Defendant's Motion for Partial Summary Judgment***

U.S. Department of Homeland Security  
Arlington, Virginia 22202



Homeland  
Security

Privacy Office DHS-D3

November 14, 2006

Mr. David L. Sobel  
Electronic Frontier Foundation  
1875 Connecticut Avenue, N.W.  
Suite 650  
Washington, D.C. 20009

Re: **DHS/OS/PRIV 07-160/ Sobel request**

Dear Mr. Sobel:

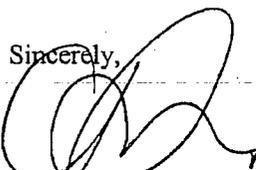
This acknowledges receipt of your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated November 7, 2006, requesting the following records concerning the Automated Targeting System (ATS):

1. All Privacy Impact Assessments prepared for the system.
2. A Memorandum of Understanding executed on or about March 9, 2005 between Customs and Border Protection (CBP) and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.
3. All records, including Privacy Act notices, which discuss or describe the use of personally-identifiable information by the CBP (or its predecessors) for purposes of screening air and sea travelers.

As it pertains to **Item 1**, please note that all Privacy Impact Assessments are made available to the public via the DHS website at [www.dhs.gov/xinfo/share/publications/editorial\\_0511.shtm](http://www.dhs.gov/xinfo/share/publications/editorial_0511.shtm). As this information has not yet been provided to DHS for inclusion on the website, we will forward this portion of your request to CBP for processing. In addition, **Items 2 and 3** are also under the purview of CBP.

I am referring your request to the Acting FOIA Officer for CBP, Rebecca Hollaway, (Mint Annex-5<sup>th</sup> Floor) 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, who will forward your request on for processing to the appropriate office within CBP. That office will issue a direct response to you.

If you need to contact our office again about this matter, please refer to **DHS/OS/PRIV 07-160/ Sobel request**.

Sincerely,  


Catherine Papoi, J.D.  
Deputy Chief FOIA Officer  
Director, Disclosure & FOIA

**Exhibit 5**

***Defendant's Motion for Partial Summary Judgment***



**Electronic Frontier Foundation**  
 Defending Freedom in the Digital World

**PROTECT YOUR RIGHTS**  
 ONLINE NOW

[About EFF](#)

[News](#)

[Press Releases](#)

[Cases](#)

[Action Center](#)

[Join EFF](#)

[Sitemap](#) | [Calendar](#)

[> Home](#) [> About](#)

## About EFF

From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990 — well before the Internet was on most people's radar — and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights.

Blending the expertise of lawyers, policy analysts, activists, and technologists, EFF achieves significant victories on behalf of consumers and the general public. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 50,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public. Sometimes just defending technologies isn't enough, so EFF also supports the development of freedom-enhancing inventions.

EFF is a donor-funded nonprofit and depends on your support to continue successfully defending your digital rights. Litigation is particularly expensive; because two-thirds of our budget comes from individual donors, every contribution is critical to helping EFF fight —and win—more cases.

**For information on donating to EFF, see**  
<http://www.eff.org/support/>

**Learn about significant EFF court victories**  
<http://www.eff.org/legal/victories/>

**Learn more about EFF's founding**  
<http://www.eff.org/about/history.php>

**Learn more about current hot cases:**

- [› AT&T Class Action](#)
- [› E-voting Florida Case](#)
- [› Diehl v. Crook](#)
- [› Zyprexa Litigation](#)
- [› Travel Screening Litigation](#)
- [› Spocko and KSFO](#)

**Learn more about EFF campaigns, projects, and issues:**

[File Sharing](#)

## Contact and Staff Information

- » [Contact Us](#)
- » [Board of Directors](#)
- » [Staff List](#)
- » [Advisory Board](#)
- » [Volunteer, Intern, and Employment Opportunities](#)
- » [How to Support the Electronic Frontier Foundation](#)

Search eff.org

Enter search terms

Powered by  
 Google

Search EFF

» [About EFF's search](#)

[EFFector](#)

**Subscribe to EFFector!**  
 [our free email newsletter]

Email:

Zip / Postal Code  
*(optional)*

Subscribe!

» [EFFector Archive](#)

Topics & Areas  
[Privacy](#)  
[Intellectual Property](#)  
[Fair Use and DRM](#)  
[Innovation](#)  
[FLAG Project](#)  
[File Sharing](#)  
[Free Speech](#)  
[Bloggers' Rights](#)  
[International](#)  
[E-voting](#)  
[Awards](#)  
[EFF Victories](#)  
[EFF White Papers](#)  
[EFF en Español](#)  
 » [Recursos e información de EFF en Español.](#)

**Support EFF's efforts through our Action Center:**

<http://action.eff.org>

To stay up to date on EFF issues, subscribe to our [EFFector](#) newsletter, or check out our weblogs, [Deep Links](#) and [miniLinks](#).

[Home](#) | [About EFF](#) | [Press Releases](#) | [News](#) | [Cases](#) | [Action Center](#) | [Join EFF](#) | [Privacy Policy](#) | [EFF RSS Feeds](#)

---

**Exhibit 6**

*Defendant's Motion for Partial Summary Judgment*



Welcome back, John Coleman.

You are subscribed to -- The following products --

[Search Results](#) | [New Search](#)

## Electronic Frontier Foundation, Inc.

Also Known As: EFF  
154 Shotwell St  
San Francisco, CA 94110



### My Tools

#### Subscribe Now

- [GuideStar Select](#)
- [GuideStar Premium](#)
- [Analyst Reports](#)
- [Charity Check](#)
- [Grant Explorer](#)
- [Data Services](#)
- [Compensation Reports](#)
- [Salary Search](#)
- [GuideStar for Grantmakers](#)
- [GuideStar Pro](#)
- [eDocs](#)

### GENERAL INFORMATION

Contact: Ms. Shari Steele  
 Telephone: (415) 436-9333  
 Fax: (415) 436-9993  
 E-mail: You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.  
 Web Site: [www.eff.org](http://www.eff.org)

#### Who We Are

The Electronic Frontier Foundation is a nonprofit public-interest organization that exists to protect and enhance our core civil liberties in the digital age. Based in San Francisco, EFF is a membership-supported organization that works on issues of free expression, freedom of press, fair use, anonymity, security, and privacy among many others, as they relate to computing and the Internet.

#### Power Searches for Professionals



Our search, sort, and retrieval options save you time and energy. [Learn more](#)

- This organization is a [501\(c\)\(3\)](#) Public Charity.
- This organization is required to file an IRS Form 990 or 990-EZ.
- Additional narrative information in this report was last supplied by the organization on January 28, 2003.
- It makes its audited financial statements available to the public upon request.
- Contributions are deductible, as provided by law.

#### How to Help

This organization is seeking funds from contributions and grants. These funds will be used for unrestricted operating expenses, special projects and endowments.

#### Location(s) Served

- National

#### NTEE Code

- R60—Civil Liberties Advocacy
- R63—Censorship, Freedom of Speech and Press Issues
- R99—Civil Rights, Social Action, and Advocacy N.E.C.

**FIN:** You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.

**Year Founded:** 1990

**Ruling Year:** 1990

**Fiscal Year:** You must be a [GuideStar Premium](#) subscriber to view this information.

**Assets:** You must be a [GuideStar Premium](#) subscriber to view this information.

**Income:** You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.

**No. of Board Members:** 9

**No. of Full-Time Employees:** 11-20

**No. of Part-Time Employees:** 0

**No. of Volunteers:** 21-100

**Chief Executive**

You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.

**Chief Executive Profile**

You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.

- [Back to Top](#)

**BOARD OF DIRECTORS**

You must be a [GuideStar Select](#) or [Premium](#) subscriber to view this information.

**MISSION AND PROGRAMS**

**Mission**

The Electronic Frontier Foundation (EFF) works in the public interest to protect fundamental civil liberties in the digital age. The Internet and other communication technologies can herald the most liberating era of human history -- or the most regulated and controlled as new threats to our basic rights to free speech, privacy and free and open communications emerge with alarming speed. Based in San Francisco, EFF is a membership-supported organization with one of the most linked-to websites in the world: <http://www.eff.org>.

**Programs**

The Electronic Frontier Foundation (EFF) works on issues of free expression, freedom of press, privacy, anonymity, security, and fair use, among many others, as they relate to computing and the Internet. EFF's objectives are to ensure that our fundamental rights are at least as well-secured online as they are offline; to educate the press, policymakers and the general public about online civil liberties; and to act as a defender of those liberties when they are attacked. Among our various activities, EFF opposes misguided legislation, defends individuals' rights in court, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, supports the development of new communication technologies, engages the press daily, and publishes a comprehensive archive of online civil liberties information on our website: <http://www.eff.org>. We pride ourselves on being the first to see potentially threatening issues on the horizon and to take pre-emptive action to protect civil liberties on the Internet.

Three of the most important legal cases of the last decade for electronic communications have been EFF cases: Steve Jackson Games v. U.S. Secret Service (email privacy), Bernstein v. U.S. Department of Justice (export controls on encryption, which defined computer code, for the first time, as a form of expression that is protected by the First Amendment), and Universal Studios, v. Reimerdes (copyright fair use).

- [Back to Top](#)
- 

## GOALS AND RESULTS

### Accomplishments for Fiscal Year Ending December 31, 2002

1. EFF has done important work in standards groups, such as the Broadcast Protection Discussion Group, a group of corporate interests negotiating a technological standard for the next generation of broadcast television, high density TV. Before EFF's involvement, the movie industry was using the group to strong-arm the computer and consumer electronics industries into a "consensus" that would have undermined fair use and other consumer rights. EFF brought this group to public scrutiny, and brought representation of the public interest to the discussion. EFF was able to make big companies think twice about consumer rights and freedom of innovation, and at the end of this process, there was no consensus on these technological standards.
2. EFF filed *Newmark v. Turner*, asking a federal court to declare that owners of the ReplayTV digital VCR have the right to digitally record television programs for later viewing, skip over commercials, and send shows to other devices. In numerous press statements and legal filings, the entertainment industry claims that such recording for "time-shifting" and "space-shifting" purposes is a copyright infringement and that avoiding commercials is "theft" and "stealing". Five ReplayTV owners, including Craig Newmark of popular San Francisco-based website Craigslist.org, have filed a Declaratory Judgment lawsuit against twenty-eight entertainment companies asking that their activity be ruled lawful fair use under copyright law.
3. EFF launched its new action center at <http://action.eff.org>, a website that educates our members on current important issues of technology, policy, and civil liberties. At the action center, members can view action alerts on technology and civil liberties issues and pending legislation where their action can make a difference. They can then take action, sending a customizable fax, email, or letter to elected leaders.

### Objectives for Fiscal Year Beginning January 1, 2003

1. Protecting the Freedom to Innovate: The entertainment industry and its lawmakers want to rob you of your freedom to own general-purpose technology. Personal computers let "consumers" do so much more than "consume", an idea that is shocking to an industry that would limit its customers to the kind of interactivity provided by a remote control. EFF is at the front of every fight to keep control of technology out of the hands of Hollywood. We will continue to expose the sham standards-bodies that write laws disguised as mandatory specifications, and lead the critical response to lawmakers who propose unconstitutional restrictions on the freedom to innovate.
2. Protecting P2P: Peer-to-peer (P2P) networks, systems that allow any two parties online to communicate without intervention or permission, reflect the natural state of the Internet. They are under continuous fire from the entertainment industry, which would have you believe that these networks have only one use, to infringe on copyright. The reality is very different. P2P networks are an exciting new way for independent artists, authors, and filmmakers to distribute their works to a massive audience outside of the traditional channels. Without EFF's defense of the Morpheus P2P system and other ongoing legal fights, the crucial principle that general purpose technology is legitimate (even if some of the uses for it aren't) would dissolve under the entertainment industry's well-funded legal assaults.
3. Protecting Your Right to Privacy: Laws like the USA PATRIOT Act undermine your privacy and freedom, granting sweeping, un-democratic powers to law enforcement agencies. EFF is a clearinghouse for information about online privacy and liberty, and we will continue to publish white-papers and advisories and to document excesses committed in the name of security.

Ongoing board/staff/advisory committee meeting to evaluate strategies and effectiveness; feedback from our "Effector" online newsletter, which has over 25,000 subscribers; feedback via our email hotline for members of the line community.

- [Back to Top](#)
- 

## FORM 990 AND EDOCS

### Forms 990 from the IRS:

- [2005 Form 990](#) 
- [2005 Form 990](#) 
- [2004 Form 990](#) 
- [2003 Form 990](#) 
- [2002 Form 990](#) 
- [2001 Form 990](#) 
- [2000 Form 990](#) 
- [1999 Form 990](#) 
- [1998 Form 990](#) 
- [1997 Form 990](#) 

### Additional Documents from the Organization:

None Available

---

## About IRS Form 990

### [Form 990 FAQs](#)

To view this organization's IRS Form 990, you must have the Adobe Acrobat Reader installed on your system. If you don't have the Reader, you can get it at the [Adobe Web site](#) for free. Having trouble viewing PDFs? [Try these steps](#).

- [Back to Top](#)
- 

## ANALYST REPORT

A GuideStar Analyst Report is available for this organization. [Learn more](#).

---

## FINANCIAL DATA

You must be a [GuideStar Premium](#) subscriber to view this information.

---

- [Back to Top](#)
- 

[Search Results](#) | [New Search](#)

**Exhibit 7**

***Defendant's Motion for Partial Summary Judgment***

---



Web Images Video News Maps more »

Iran and Nuclear and "United States

Search

Advanced news search  
Preferences

Results 1 - 10 of about 17,457 for Iran and Nuclear and United-States. (0.37 seconds)

Sorted by relevance [Sort by date](#)

Top Stories

World

U.S.

Business

Sci/Tech

Sports

Entertainment

Health

Most Popular

News Alerts

[RSS](#) | [Atom](#)  
[About Feeds](#)

[Mobile News](#)

[About](#)  
[Google News](#)



[Playfuls.com](#)

[Iran can learn from Lebanon, not N Korea](#)

Asia Times Online, Hong Kong - 6 hours ago

He also wrote "Keeping **Iran's nuclear** potential latent", Harvard International Review, and is author of **Iran's Nuclear** Program: Debating Facts Versus ...

[Bad part of Korea deal: It's not Iran](#) St. Petersburg Times

[Trudy Rubin: A reversal of policy for US](#) Dallas Morning News (subscription)

[Analysts in Tehran call Korea pact a model for Iran](#) San Francisco Chronicle

[Playfuls.com - International Herald Tribune](#)

[all 96 news articles »](#)

[US puts squeeze on 3 Iranian firms](#)

San Jose Mercury News, CA - 32 minutes ago

It marked the government's latest move to put the financial squeeze on **Iran**, a country the **United States** accuses of fostering terrorism and whose **nuclear** ...



[Playfuls.com](#)

[US must keep pressure on Iran, but time isn't right for bombing](#)

San Jose Mercury News, CA - 5 hours ago

At the same time, we need to remind the gulf monarchies that a **nuclear** Shiite theocracy is far more dangerous to them than either the **United States** or ...

[Tapping Ahmadinejad's egg](#) Town Hall

[Growing Fear of Nuclear Iran](#) Citizen Journalism Nepal

[Iran official hints at halting atomic work: report](#) National Post

[Kommersant](#)

[all 77 news articles »](#)



[Beyond Chron](#)

[Israel's Bomb, Iran's Pursuit of the Bomb and US War Preparations ...](#)

OpEdNews, PA - 10 hours ago

Indeed, Israeli intelligence has provided both the **United States** and the IAEA with accurate intelligence about elements of **Iran's nuclear** program, ...

[Crying Nuke](#) American Spectator

[Apply the lessons of Iraq to Iran](#) Belleville News-Democrat

[No George, No Iran](#) Huffington Post

[Angus Reid Global Monitor - Spero News](#)

[all 109 news articles »](#)



[Boston Globe](#)

[Asia: North Korea Seen As Seeking Diplomatic Gains From Nuclear ...](#)

RadioFreeEurope/RadioLiberty, Czech Republic - 2 hours ago

Further afield, US officials have said that the Korean deal could serve as a model for solving the **nuclear** crisis between **Iran** and the international ...

[The Strange North Korea Deal](#) John Birch Society

[A willingness to talk](#) Toledo Blade

[Talking point](#) Fort Worth Star Telegram

[People's Weekly World - Al-Ahram Weekly](#)

[all 1,102 news articles »](#)



[E Canada Now](#)

[According to Putin, US Is the Bigger Threat](#)

Washington Post, DC - 22 hours ago

Since it's hard to tell exactly when it will become a reality and how it will affect the world, it is tempting to wave off a **nuclear Iran** and go on blaming ...

[Bush Downplays Rift With Russia](#) St.Petersburg Times.ru

[Bush seeks cooperation with Russia despite Putin's harsh remarks](#) Pravda

[Bush: Putin relationship complicated, common goals](#) Journal of Turkish Weekly

[Xinhua](#)

[all 99 news articles »](#)

[Bad deal is worse than no deal](#)

AZ Central.com, AZ - 9 hours ago

North Korea calculated, correctly, that having a **nuclear** weapon was an effective deterrent against a conventional military threat by the **United States**. ...

[How deal on Korea nuclear program was cut](#) Bush, Kim Jong Il both ... San Francisco Chronicle

[all 94 news articles »](#)



[Washington Post](#)

[US, developing nations accept Iran aid cut plan](#)

San Diego Union Tribune, CA - 25 minutes ago

But members ranging from **Iran's** arch-foe the **United States** to its close ally Cuba raised no objections when IAEA aides, at a briefing this week, ...

[EBaradei says US must engage Iran](#) Scotsman  
[all 193 news articles »](#)



[Playfuls.com](#)

[Russia Expects US Flexibility with Iran as shown with North Korea](#)

Center for Research on Globalization, Canada - 13 hours ago  
Russia expects the **United States** to show the same flexibility in resolving the problem of **Iran's nuclear** program as it did with North Korea, ...

[Russia Expects US Flexibility on Iran as on Korea](#) Fars News Agency

[Russia calls for similar US 'flexibility' on Iran as on NKorea](#) Hindu

[Russia expects US flexibility on Iran as on N.Korea](#) ABC News

[all 32 news articles »](#)



[Raw Story](#)

[The Rogue Weasels](#)

FrontPage magazine.com, CA - 8 hours ago

The US was also expected to acquiesce to **Iran's nuclear** programs. And all this, was supposed to usher in Peace in Our Time. There are too many problems with ...

[Former NSC Official Contradicts Rice on Iran Peace Offer](#) Kansas City infoZine

[Would Your Government Lie To You? Across the Aisle](#)

[Ex-aide says Rice misled Congress on Iran](#) IranMania News

[Journal of Turkish Weekly - Swissinfo](#)

[all 30 news articles »](#)

New! More ways to find the latest on **Iran and Nuclear and United-States**:

- [Search blogs](#)
- [Create an email alert](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

Iran and Nuclear and "United States"

**Exhibit 8**

***Defendant's Motion for Partial Summary Judgment***



Web Images Video News Maps more »

Surge and Iraq

Search

Advanced news search  
Preferences

Results 1 - 10 of about 15,142 for **Surge and Iraq**. (1.15 seconds)

Sorted by relevance [Sort by date](#)

Top Stories

World

U.S.

Business

Sci/Tech

Sports

Entertainment

Health

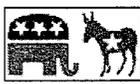
Most Popular

News Alerts

[RSS](#) | [Atom](#)  
[About Feeds](#)

[Mobile News](#)

[About](#)  
[Google News](#)



WHDH-TV

**House set to vote on troop surge in Iraq**

Virginian Pilot, VA - 10 hours ago

Thelma Drake, R-2nd District, took pains to distance themselves from the troop surge as they urged defeat of the resolution. ...

[US House is expected to vote on President's troop surge today](#) WBIR-TV

[Forum Editorial: Iraq war resolution is pointless](#) In-Forum (subscription)

[Follow the Iraq resolutions with benchmarks for Bush](#) USA Today

[FOX News - Virginian Pilot](#)

[all 2,858 news articles »](#)



Fox 28

**US House To Vote On Iraq Resolution**

HULIQ, NC - 27 minutes ago

The US House of Representatives is expected to vote later today on a nonbinding resolution to oppose President George W. Bush's troop surge for Iraq. ...

[Senator Biden: 2002 Iraq War Resolution No Longer Relevant](#)

[All American Patriots \(press release\)](#)

[DEMS FOR A TERROR HAVEN](#) New York Post

[Biden Favors Revised Iraq War Resolution, Promotes Partition Plan](#) New York Times

[Delmarva Daily Times](#)

[all 142 news articles »](#)



Pittsburgh Post  
Gazette

**Murtha Touts New Way to Stop Troop 'Surge' in Iraq**

Crosswalk.com, VA - 7 hours ago

plans to introduce legislation designed to halt the Bush administration's troop "surge" in Iraq by restricting military deployments - a move he is painting ...

[Abercrombie, Hirono speak against troop surge](#) Honolulu Advertiser

[Murtha gears up for legislative battle on Iraq war funding](#) Pittsburgh Post Gazette

[Hawaii delegation criticizes Iraq war](#) Honolulu Star-Bulletin

[all 12 news articles »](#)



HNN

Huntingtonnews.net

**Capito speaks against resolution critical of Iraq troop surge**

Daily Mail - Charleston, WV - 4 hours ago

Despite her initial opposition to a troop surge in Iraq, Rep. Shelley Moore Capito is siding with most House Republicans by voting against a resolution that ...

[Capito Opposes Troop 'Surge.' Also Opposes Democratic Iraq ...](#) HNN Huntingtonnews.net

[EDITORIAL: Capito Has Her Cake, Eats It, Too, and Then Some](#) HNN Huntingtonnews.net

[Capito comments on troop resolution](#) Martinsburg Journal

[all 6 news articles »](#)



Javno.hr

**Another Surge?**

Slate - 17 hours ago

Politics/entertainment blog The Darkefang Post colored the plan politically: "He's combining the surge in Iraq - which has lukewarm support at best - with a ...

[Bush on Afghanistan: Another Surge, a Renewed Offensive](#) Mother Jones

[Bush calls for Afghanistan 'surge' even though 'remarkable ...](#) Raw Story

[Bush Announces More Troops For Afghanistan](#) HULIQ

[Free Internet Press - DetNews.com](#)

[all 637 news articles »](#)

**Petri against troop surge**

Appleton Post Crescent, WI - 6 hours ago

In an interview after his speech, Petri said he felt it was important to offer a suggestion for a resolution of the Iraq war to provide a basis for his vote ...

[Petri plans to oppose troop surge in Iraq](#) Milwaukee Journal Sentinel (subscription)

[Petri joins opposition to Iraq buildup, wants to partition](#) Oshkosh Northwestern

[all 7 news articles »](#)

**Iraq war draws nays in state capitols**

Stateline.org, DC - 11 hours ago

16) on a nonbinding resolution against Bush's plans for a troop surge in Iraq. But the first legislative bodies in the nation to lash out at the war were ...



**US Troop Surge in Iraq**

American Chronicle, CA - Feb 14, 2007

Many hardcore supporters of the Iraq War policy have also supported increasing the number of US troops in Iraq and what is now termed a troop surge - a plan ...



**Exhibit 9**

***Defendant's Motion for Partial Summary Judgment***



[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

cricket and match

Search

[Advanced news search](#)  
[Preferences](#)

Results 1 - 10 of about 11,547 for **cricket and match**. (0.65 seconds)

Sorted by **relevance** [Sort by date](#)

Top Stories

World

[Have you stopped channel surfing on a \*\*cricket match\*\* and wondered ...](#)

Toronto Sun, Canada - 7 hours ago

U.S.

Business

This is **Cricket 101**. **Cricket For Dummies**. Just in time for the India vs. Pakistan all-star **match** at Rogers Centre March 3. And for the World Cup, ...

Sci/Tech

Sports

Entertainment

Health

Most Popular

[News Alerts](#)

[RSS](#) | [Atom](#)

[About Feeds](#)

[Mobile News](#)

[About](#)

[Google News](#)



Kenya London News

[Kenyan officials settle pay row with \*\*cricket\*\* World Cup players](#)

Reuters South Africa, South Africa - 1 hour ago

"They agreed to pay us fees for the **match** against Canada which we were awarded after six of their players fell sick in Mombasa last month," Tikolo told ...

[Players stage sit-in at \*\*Cricket\*\* Kenya headquarters](#) CricInfo.com

[Kenyan officials settle pay-row with World Cup players](#) Zee News

[Cricket Kenya now sets aside Sh7.2m for players](#) Standard

[Capital FM](#)

[all 18 news articles »](#)

[Cricket trophy up for grabs this weekend](#)

Wairarapa Times Age, New Zealand - 12 hours ago

The annual **cricket** "test **match**" between Wairarapa College and Rathkeale College will be played at Queen Elizabeth Park oval in Masterton tomorrow and Sunday ...

[Arsenal-Bolton \*\*Match\*\*](#)

WagerWeb, Costa Rica - 1 hour ago

Author Bio: Tim is a UK-based sports journalist specializing in European football, **cricket** and North American sports. Having been raised on football and ...



BBC Sport

[Ponting's poser: Are weary Australia suffering from too much \*\*cricket\*\*](#)

Sportingo, Israel - 25 minutes ago

Australia have played so much one-day **cricket** in the last month that they have dropped out of form at the worst possible time. Friday's **match** was their 11th ...

[Australia could lose top one-day spot for first time](#) Khaleej Times

[Proteas on top of the world AND](#)

[SA now joint leaders in ODI standings](#) Supersport

[Sunday Times](#)

[all 35 news articles »](#)

[CRICKET - Southee bolts into ND gap left by Tuffey](#)

Northern Advocate, New Zealand - 11 hours ago

Although Southee has already played for ND in a warm-up **match** against Auckland and in a Twenty20 **match** against Central Districts, he admits he is still a ...

[Southee gets his chance of ND debut after 20-wicket test haul](#) Waikato Times

[all 3 news articles »](#)



Gulf News

[Cricket: Samuels Named In Windies World Cup Squad](#)

Hardbeatnews.com, NY - 13 hours ago

The Samuels scandal comes some seven years after a **match**-fixing scandal that led to a life ban from **cricket** for the late Hansie Cronje, then South African ...

[Bowled over by betting rows](#) Gulf Weekly

[Should a bookmaker be on the \*\*cricket\*\* board?](#) Stabroek News

[Samuels in World Cup squad despite probe](#) Jamaica Gleaner

[The Australian - Nation News](#)

[all 116 news articles »](#)



BBC Sport

[Cricket's credibility takes a hit](#)

The Australian, Australia - 1 hour ago

THE Chappell-Hadlee Trophy degenerated into farce when Michael Clarke became the fourth member of Australia's top five to be unavailable for the first **match** ...

[Australia suffers first ever \*\*cricket\*\* ten wicket loss](#) Radio Australia

[Credibility first casualty of schedule](#) The Australian

[Lee gives Aussies a jolt on eve of final shake-down series](#) Business Day

[Bloomberg - Gulf Daily News](#)

[all 158 news articles »](#)

[New Zealand seeks World Cup boost in Chappell-Hadlee series versus ...](#)

SLAM! Sports, Canada - 12 hours ago

WELLINGTON, New Zealand (AP) - New Zealand will test critical elements of its World Cup



Gulf News

armoury in its three-match Chappell-Hadlee limited-overs cricket ...  
[New Zealand seek CWC boost in ODI](#) Supersport  
[New Zealand seeks World Cup boost in Chappell-Hadlee series](#) Indiatimes  
[Australia, New Zealand Name Cricket Squads](#) OhmyNews International  
[all 18 news articles »](#)



Sydney Morning Herald

**Cricket: Fleming digs in against the bouncers**  
New Zealand Herald, New Zealand - 25 minutes ago  
Fleming said he was particularly surprised to see his post-match comments from Brisbane twisted around to suggest he wasn't particularly bothered about ...  
[Fleming Shrugs Off Criticism](#) Xtra News  
[Your Views: Cricket: NZ's woes?](#) New Zealand Herald  
[Black Caps humiliate Aussies](#) SkySports  
[The Press - CricInfo.com](#)  
[all 19 news articles »](#)

New! More ways to find the latest on **cricket and match**:

- [Search blogs](#)
- [Create an email alert](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

cricket and match

Search

**Exhibit 10**

***Defendant's Motion for Partial Summary Judgment***

---

**U.S. DEPARTMENT of STATE****End-of-Year Review****Daniel Fried, Assistant Secretary for European and Eurasian Affairs**Press Roundtable  
Washington, DC  
December 12, 2006

**Assistant Secretary Fried:** End-of-year wrap-ups are rather artificial things, but I will use as a starting point the recent end of year ministerials and summit from which I've just returned: the NATO Summit in Riga; the Forum for the Future ministerial in the Dead Sea, Jordan; and the OSCE [The Organization for Security and Cooperation in Europe] Ministerial in Brussels. The reason I chose these, other than the fact that I've just returned so it's fresh, is because it shows that the U.S.-European relationship is developing well and is in action out in the world in ways that the readers of many of your publications may not be aware and American publications may not be aware, given the intense and sometimes exclusive focus on Iraq. This isn't to say Iraq isn't important, but there are other things in addition that are happening.

The U.S.-European relationship, unlike the days of the Cold War, is not concerned with itself or with threats to Europe from within Europe or from the periphery of Europe, which was the case in the Cold War. The U.S.-European relationship is concerned with far-flung areas around the world. This is where the problems are; this is where the opportunities are to advance freedom, security, prosperity.

The United States and Europe are busy developing the bases of a relationship in which these two great centers of democratic legitimacy in the world are working together to advance our interests and our values in working with partners around the world. That's a very general statement, but it is actually one with considerable basis in hard reality.

At the NATO Summit, the NATO leaders talked about NATO's challenges in support of the Afghan people. Now if on September 10, 2001, anyone had dared to write a policy paper or a story about NATO going into Afghanistan, it would have been dismissed as utterly ludicrous. Now this is reality. I mention this only to show how much has occurred in the past five years and how much has been achieved in reorienting the U.S.-European relationship from a close-in and inner-directed focus to an outer-directed, far-flung focus.

At the Forum for the Future, ministers from the region, ministers from Europe and civil society groups from across the Middle East met to support reform and democracy. I emphasize this because it is often overlooked that there is a demand in the region, in the Middle East, the broader Middle East, for reform and democracy. And it is often overlooked that there is a U.S.-European consensus that we should be supporting these voices that call for change.

It is too often an assumed cliché that support for reform in this region is either futile, because it will lead to nothing, or dangerous, because if it leads to anything at all it will be some kind of extremism, but, in fact, the civil society groups from the region said again and again, "We want reform, we want greater emphasis on the rule of law, we want more democracy." Here, overlooked by many, is a European-American consensus that we should be supporting these voices, these groups.

Finally, at the OSCE the United States and Europe worked together in an attempt, I'm afraid unsuccessful, to support OSCE efforts in the so-called frozen conflicts in Georgia and Transnistria, but we worked together successfully, as it turned out, and happily with Russia to defend the prerogatives of ODIHR [Office for Democratic Institutions and Human Rights], OSCE's unique, effective election monitoring instrument. This showed that Europe and the United States take seriously our responsibilities to work with the OSCE to advance democracy, democratic values across all of Europe, and, in particular, the places where democracy is the least advanced and therefore needs the most help. So the year ends with a lot of common U.S.-European activity rooted in a common agenda.

Now no doubt many of your questions will be about Iraq and the Iraq Study Group Report, so let me simply say that the administration is studying this intensely, as is public knowledge. The President is taking the recommendations seriously, of course, listening to those in the administration and outside of the administration, collecting views. The President will make his decisions about the course in Iraq. I haven't said anything particularly new, but I will say that it's clear from, and it was clear to me listening to the President's speech at Riga, that the President is committed both to help the Iraqi people and committed to help the forces of freedom and reform throughout the broader Middle East. We have a responsibility not to abandon them and a responsibility to seek to get this right.

There is obviously a great deal more we could discuss, and I'm sure your questions will bring out more on these issues and many others, but I want to emphasize that I end the year satisfied with what we've achieved in U.S.-European relations.

I'm pleased by NATO's outward-looking focus, by its outreach to countries of the Middle East, by its acknowledgement that its responsibilities are far-flung.

I'm pleased by the relationship developing between the United States and the European Union. A strong NATO doesn't mean a weak EU. Quite the contrary, we want our partners, all of them, to be strong. All of them to be strong.

It was a difficult year in many ways, but it was also a year in which democracy consolidated itself and advanced in Georgia. A year in which Ukraine may have stabilized its politics and hopefully will find a way forward. I certainly hope so. It's a year in which the international community, the United States and Europe in the lead, have been working to resolve the issues of Kosovo final status, and I think this will be one of the major issues of 2007.

A year of hard work lies ahead, a year of hard work has ended, but I see the United States and Europe working together in a difficult world, but a world of promise.

I will stop there and take your questions.

**Question:** For months there have been talks about Turkey joining the EU, [inaudible]. And the British Foreign Secretary said yesterday that the train was still on the track at the end of the meeting of the EU Foreign Ministers in Brussels. But the Minister said he agreed to punish Turkey for refusing to open its ports and airports to Cyprus and EU members. How do you evaluate those recent developments? Is this a serious setback in terms of Turkey's EU membership process? And are you worried that Turkey might go to the other direction and become more religious if the EU process is [inaudible]?

**Assistant Secretary Fried:** We have followed very closely relations between the European Union and Turkey. The views of my government and of President Bush are very clear. We certainly support Turkey's aspirations to join the European Union. We have for some time, and we have said so. We have always believed that Turkey

had to meet the European Union's criteria, and we've said this is a matter for Turkey to work out with the European Union.

Of course the particular issues of Cyprus are complicated in themselves and then as they impact the process between Turkey and the EU, that's complicated even more.

We hope that the decisions of the European Council, the European Union about the way ahead will work out in a way that allows this process to continue. It's important that it does.

I'm not going to comment on the specifics. For one thing, these discussions are still in motion, and there are many things I could say, many things the United States could say that would not help the process, so I will let caution be my watchword in describing this.

But I think if we step back and look at this more broadly, Turkey is undergoing a profound democratic transformation. The Turkey of the '60s, '70s, '80s is in the past. Turkey is, of course, and remains a secular republic, but it is one in which democracy is deepening. Reforms are changing the country. This process is going in complicated ways, as these reform processes tend to be, but I look at Turkey as having enormous potential to become a country with both deep democratic roots, a country with a mostly Muslim population which demonstrates the essential falsehood of the charge - that spurious and I think deeply insulting charge - that somehow Islam and democracy are incompatible or that one cannot have a secular republic plus respect for religion. I think these things are indeed compatible and I think Islam is no different than any other religion in this respect. So I have enormous respect for Turkey's potential and also respect for the process between the EU and Turkey, and I hope this succeeds.

**Question:** I had a question on Kosovo. Kosovo is an issue that is a worry, especially for the Europeans. Can you tell us what is the final position of the United States on the final status of Kosovo?

**Assistant Secretary Fried:** We support Martti Ahtisaari's mission, which is to develop recommendations for the Security Council on Kosovo's final status. I don't think I should comment about what we think the final status should be except to say that we have enormous confidence in President Ahtisaari. We also think that the people of the Balkans need clarity about the future and the way ahead. They need and deserve a clear road to Europe. They need and deserve leaders who will take them from the past into a better future for the 21<sup>st</sup> Century.

Kosovo has been essentially run by the United Nations since 1999 and the Kosovars deserve clarity about their future.

NATO recently made the decision to offer Partnership for Peace for Serbia. This was done despite the fact that Ratko Mladic is still at large, but despite that fact NATO determined that it would be in the interests of Europe, in the interests of the region, to make clear to Serbia and to Serbs that they did have a future with Europe. This was a decision, I believe, Greece championed early, and after consulting with many countries we, the United States, determined this was the right way forward, and we made this decision. But Serbia needs to break with its past and it needs to embrace a European future.

I'm sorry that we all face the choices that we're going to face in 2007. There was a better way, but Milosevic destroyed old Yugoslavia and we must make the most of the circumstances of the time in which we're set.

**Question:** I'm going to be very Anglo-centric and ask about the imminence of the post-Blair era, your view, if I may, about how relations with Britain will change when Tony Blair departs we think next summer. Also what was the reaction inside the State Department [inaudible] to the recent speech by David Cameron, the British Conservative leader, on the special relationship where he identified himself as liberal conservative rather than neo conservative, which is seen as distancing himself from this administration in every way he could.

**Assistant Secretary Fried:** Neo conservative, liberal conservative. Labels that have more emotional than intellectual content, I'm sure. These things are cast about.

I think Americans generally have the highest regard for Tony Blair. He's one of the most respected world leaders in the United States, and this is without regard to party - Democrats, Republicans, independents. All respect Tony Blair.

I certainly am not going to comment about the future of U.S.-British relations except to say I don't doubt that we will work closely with the next British Prime Minister, whoever that is, whenever that is. But there is no doubt that Tony Blair enjoys esteem and respect almost universally in the United States.

I'm certainly not going to comment or characterize any particular speech of opposition leaders or otherwise. We've dealt with British governments, the British have dealt with American governments, we will continue to deal with each other.

**Question:** When you say Tony Blair is held in such high regard and esteem and respect across the United States, that's almost unique [inaudible] among foreign leaders. His departure must change something in that foreign relationship because whoever is coming in will not have that same personal relationship, will not have that same esteem and respect.

**Assistant Secretary Fried:** Well, to say that we regard the Prime Minister with the esteem with which we regard him is not to make a prediction about the future. I think I understand what you're trying to do, and nice try. [Laughter]. But we will work with the next Prime Minister. But I will simply state my own view and my characterization - that Tony Blair enjoys the highest respect and he has done great things for the world, as well as for the U.S.-British relationship. I know that there will be a vigorous - in fact, there is a vigorous debate in the UK - but it's not my place to comment on it.

**Question:** I wanted to ask about Russia. In the recent briefing you made an interesting comment quoting Mark Twain which could only mean that the relations with Russia are as bad as they are depicted in the American press. Is that really how you view the relationship after Hanoi, after Moscow, meetings between our leaders?

**Assistant Secretary Fried:** I can't imagine what quote you're referring to.

**Question:** You said that, you were asked, might the relations be actually better than we think? And you said it reminds me of the quote of Mark Twain about Wagner, the music of Wagner, that it's better than it sounds. [Laughter].

**Assistant Secretary Fried:** It is true that Presidents Bush and Putin had a very good meeting in Hanoi. I was not there, but all accounts suggest it was a good meeting. They are able on a personal basis, they have strong relations and they're able to work together and to speak honestly and openly, and this has been important, as we have a number of important issues to work on with Russia and cooperate with Russia about.

We cooperate with Russia very well on a number of issues. For instance, nuclear non-proliferation. For example, North Korea. We have worked well, so far at least, on Kosovo in the Contact Group. Our economic cooperation has recently advanced because of the conclusion of the WTO bilateral. Of course it will be in everyone's interest to see Russia join the WTO. There are other issues where we have had disagreements, and we're able to discuss these in a straightforward and respectful

manner and we will continue to do so.

It's always important to remember that U.S.-Russia relations now, the disagreements notwithstanding, cover some of the world's most important issues, and we look forward to working with Russia wherever we can. When we disagree, we will deal with that issue by issue.

**Question:** And you used to say - not necessarily you, personally, but the U.S. officials used to say, including Secretary Rice, even when she was the National Security Adviser - that for the U.S. the concern with Russia is not its strengths but rather its weaknesses. Does that opinion still stand?

**Assistant Secretary Fried:** I would put it this way. We want to see a strong Russia, but a strong Russia strong in the measures of national strength which ought to count in the 21<sup>st</sup> Century. 19<sup>th</sup> Century strength was rooted in balance of power and domination of neighbors. 21<sup>st</sup> Century strength is derived from a strong free market economy, from strong democratic institutions, and we want to see a Russia strong in all of these measures.

A weak Russia does nothing for us. A strong Russia at peace with itself, at peace with its neighbors, able to contribute to the resolution of world problems is a Russia that we welcome and look forward to working with.

**Question:** Can I ask about Russian neighbors?

**Assistant Secretary Fried:** We can come back.

**Question:** All the four Visegrad countries - Poland, the Czech Republic, Slovakia and Hungary - seem to have their share of trouble lately. Is it in the region a course of popular concern for you, and is the United States trying to have them to ease the tensions inside those countries?

**Assistant Secretary Fried:** I have to tell you that when I look out on the problems of the world and I look at Central Europe and where the democratic transformations began in 1989, I still look at a region which has undergone a profound historic success.

Yeah, politics is rough. Who said it wouldn't be? But the countries, the Visegrad countries have traveled a tremendous distance and done very very well indeed.

What the United States did in the 1980s in supporting democracy, we did so so we would not have to worry about the domestic politics. We wouldn't have to think about the results of elections as being critical. It's up to the Hungarians and the Poles and the Czechs and the Slovaks. You're sovereign countries, you're democracies, you're in NATO, you're in the European Union. You'll figure out your own answers.

I'm glad that we supported democracy in your countries when we did, but everything we did, we did so you would be sovereign democracies and contributing members of the international community, and you've succeeded.

There are still some issues that the Visegrad countries have urged the United States to address, like visa issues, and as you heard the President in Tallinn, we're taking steps to resolve that as well.

**Question:** A question concerning the 800- pound gorilla who is still in the room and has been quiet. After the release of the Iraq Study Group Report, there's kind of a holiday spirit of bipartisanship in the U.S. it seems. Do you foresee something like more of the spirit of bipartisanship also between Europe and the U.S. after taking into consideration that the Iraq War has been a big spoiler of transatlantic relations?

**Assistant Secretary Fried:** I think that European governments certainly do not want to see the democratically elected Iraqi government fail. I think they want that government to succeed. This is without prejudice to the positions of particular governments about the decision to overthrow Saddam Hussein.

There is almost universal desire that things will work out better in Iraq, and I sense that European governments aren't trying to score points; they're trying to help resolve problems. So I think as a narrow answer to your question, yeah, I think there will be a serious effort by Europeans to work with us to help solve the problems. I think that Europeans want to see where President Bush will come out as he reviews both the conclusions of the Iraq Study Group and reviews other advice that he's gotten.

I also sense, and I've felt this for some time, that the acute divisions between the United States and some European countries over Iraq have faded. This has certainly been the case, and I think if I had to analyze the turning point it would be the President's February 2005 trip to Brussels, where he met with NATO and he met with the European Council and made it clear that the United States wants a strong Europe as a partner and a strong European Union, as well as a strong NATO.

Starting with that, I sense that European governments also reached back to President Bush and the American government, and there has been a sense of cooperation. There are issues on which we will differ with Europe, but alliance and friendship doesn't mean unanimity on all issues.

I think that Europe is serious about working with us, working together to solve problems, and I want to build on that spirit in the coming year.

**Question:** Don't you think there's still a sense of vindication at least in large majorities of the population I think in all European countries that actually they were right and the U.S. has been wrong on the Iraq War? If that's true, and I think it's true, what could the State Department do, especially in terms of outreach, to convince publics in Europe that, well, it's time to look into the future in terms of scoring points.

**Assistant Secretary Fried:** Look, I don't sense that governments are scoring points. I think that the experience in Iraq is what it is. Obviously we wish things had gone better than they have. On the other hand, Saddam Hussein is no more - no more in charge of that country.

I think that European publics see Iraq as it is and they want to see a better solution. I don't sense that European publics are interested in scoring points. The occasional politician or publicist may be, but that's just a price of doing business in democracies. My sense is that Europeans, despite the disagreements, want to work with the United States in common cause. It does no good to score points or just get stuck in an endlessly circular argument, and I think there is a willingness in Europe, as in the United States, to put the debate about Iraq where it belongs, which is in the past, and work to try to get Iraq and other issues right.

**Question:** On the Afghanistan issue, were you satisfied by the degree to which European nations were willing to provide more troops for the mission there?

**Assistant Secretary Fried:** Well, the NATO Summit featured a lot of discussion about Afghanistan. European governments, European nations have contributed impressively to the common mission in Afghanistan. Some European governments have troops that were fighting in the south in the summer and early fall. Some of them suffered significant casualties, and we should remember that: the Canadians, the British, others down in the south, as well as the Americans. Some governments have been doing a good job in the north; the Germans in Kunduz. When the NATO commander asked for more troops, the Poles came forward very quickly with the offer of a mechanized battalion without caveats. That is enormously impressive. Poland has a serious military, and they know what they're doing.

So countries have made contributions. Now, do we think the so-called caveats, the restrictions, should be lifted? Of course we do. Of course we do. But that doesn't mean we have scant regard for the contributions of countries, of all the countries that have troops in Afghanistan. We understand this is hard for some governments and some parliaments. So we want to see governments commit themselves to a common mission, commit themselves to success. We are working not just on the military side of this, because success in Afghanistan is not just military, it isn't even primarily military; it's political, it's social, it's economic, it's information, and we need to get our strategy right and succeed for the sake of the Afghan people.

In NATO, my sense was governments are serious about that, and we will be working with this in the New Year.

**Question:** You talked about reform in the greater Middle East. To what degree does this administration think that the problems in Iraq have also created problems for the moderates in other Arab states who want to go on to reform some of these states?

**Assistant Secretary Fried:** The Middle East of let us say the '70s and the '80s, of authoritarian regimes, is gone. What is emerging is a Middle East of ferment, turmoil, in some cases terrible things. I don't want to make a rosy picture of this. But also of a demand for reform and democracy and justice. And it's important. The reason I mentioned the Forum for the Future is that it is important not to forget those voices, those forces in the region who believe in democracy, who believe in reform, and in the rule of law, and not reduce the region to stereotypes of authoritarians or extremists.

It is too easy to do that, and that would be a grave insult to the people who at sometimes at great risk to themselves stand for values which are not actually Western, but are universal.

To answer your question, obviously the sectarian violence in Iraq and in Baghdad in particular is troubling both in itself - people are being killed. That is greatly troubling, obviously. But it also is the success of extremism, of purveyors of violence and the ideologues who inspire them, is a challenge. President Bush said so very clearly, better than I have, in his speech in Riga. It's important to get behind the forces of reform and positive change, and it is a contest in which we cannot be neutral or indifferent. We have to help the forces of reform succeed.

Obviously progress in one area helps reformers everywhere, and it's important to advance on a broad front as best you can.

I think there is an understanding in Europe that we have to work together to help reformers in this region solve the problems. That is one of the, in fact it is probably the chief item on the U.S.-European agenda today.

**Question:** But do you think their job is harder now than it used to be?

**Assistant Secretary Fried:** Well, it depends on what you mean by used to be. We obviously hope that the sectarian violence is suppressed and that Iraq moves in a better direction. We obviously hope that as it does the reformers in the region will be strengthened. But it's wrong, I think, to draw too mechanistic a parallel. I think also individual situations in countries vary rather widely. But it is important that Iraq succeed, and you can make an argument - we have made the argument - that success in Iraq will make a major difference throughout the region.

I'll take your principle point because that has a certain validity to it. Not to make it too mechanistic, but yeah, it's important to succeed in Iraq.

**Question:** Donald Rumsfeld, the soon to be ex-Defense Secretary, once divided Europe into old and new. Do you think those terms have any meaning these days? Particularly when you look at [inaudible] Iraq and the Middle East. It appears that old Europe [inaudible] strong. Perhaps your greatest ally now with regard to actually [inaudible].

**Assistant Secretary Fried:** You brought up the old and new. You haven't heard that from anybody in the administration in some time. I think those remarks have been over-analyzed and certainly we're not interested in dividing Europe. We want to work with all of Europe. We look forward to doing so. We look to Europe and we look to our friends in Europe and want to work cooperatively and on a common agenda.

**Question:** Just one point about Syria and France.

**Assistant Secretary Fried:** Well, it is certainly true that we've been working very closely with France on Lebanon and by extension on the problem that Syria constitutes. We've been working very closely. Presidents Bush and Chirac helped launch this effort in their February 2005 dinner in Brussels. That was an important dinner. We've been working very closely with the French. It sort of demonstrates my point.

**Question:** There is a sense that [inaudible] Syria. One is they can be flipped [inaudible]. The other view is that [inaudible] increase their [inaudible]. On that you seem to be closer to France than you do to say perhaps [inaudible].

**Assistant Secretary Fried:** Look, I'm not going to comment on individuals because I can see the way that might appear.

Nigel Sheinwald, the Diplomatic National Security Advisor of Great Britain, went to Damascus at the end of October, and he delivered a very clear message. After that there was another political murder in Beirut. So figure out what that means.

If Syria wants for its own reasons to contribute to a resolution or stabilization of Iraq, it can do so, it knows how. If the price it seeks is a free hand in Lebanon, no deal. I think that's a very important message for the Syrians.

**Question:** A question regarding Kosovo again. How big do you think are the chances to find a solution within the UN, as long as Russia is against an independent Kosovo?

**Assistant Secretary Fried:** Well, we need a solution. I don't want to speculate about the prospects in the United Nations, but Russia knows; Russia's experts on Kosovo are very good indeed. These are serious people. They know the ground. They have made a very strong and convincing case that whatever the final status in Kosovo, the historic Serbian community needs to be protected. That is the monasteries, the Serb communities that are still there, both north and south of the Ibar. There needs to be decentralization. So Russia has played, as I've said, a very constructive role in that regard. Russia understands that the status quo in Kosovo is not sustainable, that we can't go back to the situation before 1999. The only way out is forward, and I hope Russia will continue to see this through to the end in the interests of a stable Balkans, a Serbia with a future, and a future for the people of Kosovo, all of them; which is better than the past. I certainly hope Russia sees it that way, and they have some very capable people who can play a major role in seeing this through.

**Question:** Again on Kosovo, please. There are some reports that the U.S. government is opposed to conditional independence. Can you -

**Assistant Secretary Fried:** I don't know what the term means. Never heard it, doesn't exist. Either you're independent or you're not.

Question: What is -

**Assistant Secretary Fried:** Look, I'm not going to get into the particular position that we have, or that Ahtisaari will have, but no, not conditional independence. The term doesn't arise. Ahtisaari will finalize his recommendations, he'll make them, we'll see how that comes out and we will return to this issue.

Question: There was limited sovereignty under Brezhnev.

**Assistant Secretary Fried:** I wouldn't cite Brezhnev as a model [Laughter]. You're free to do so, of course.

Question: May I ask about NATO, Ukraine and Georgia. What next steps do you see in terms of bringing Georgia into NATO?

**Assistant Secretary Fried:** This is going to be a process that will not unfold tomorrow. Our view is that NATO's door should remain open for countries that are both willing to join NATO, eager to join NATO, and meet NATO standards. That process is just beginning. Ukraine doesn't seem to me to yet have a national consensus about NATO membership. Georgia seems to have a national consensus. They have a way to go. So let's take this a step at a time.

Right now Georgia is properly focused on strengthening its economy, strengthening its democratic institutions, peacefully resolving the issue with the frozen conflicts. Those are very good priorities for Georgia. We support Georgia's sovereignty, we support its right to determine its own future, and as I said to my Polish and Visegrad friends 15 years ago, as these countries take care of their internal reforms the external arrangements will take care of themselves. They didn't believe me at the time, but maybe they'll think better of their earlier skepticism.

Question: Actually, to build upon this, the Georgian Prime Minister is here. Doing exactly what you just mentioned. Did you really discuss with him a free trade zone? A U.S.-Georgia free trade zone, as they report, the Georgians?

**Assistant Secretary Fried:** We've discussed U.S.-Georgia economic relations. He's meeting the Vice President this afternoon, and I don't want to preview that message. There are a lot of ideas floating around. We certainly think that the Prime Minister's message about economic reform, about opening new markets for Georgian products since Russians are now deprived of the centuries-old pleasure of drinking Georgian wine, I frankly will be happy to find more of it in my local store. It's quite good, by the way.

Question: I know.

**Assistant Secretary Fried:** But your children will not, unless things change.

Question: They will.

**Assistant Secretary Fried:** Last question.

Question: I need to ask my German question because -

**Assistant Secretary Fried:** Go ahead.

Question: EU presidency and G8 presidency is coming up. What does it mean in terms of Germany?

**Assistant Secretary Fried:** Look, it's a great chance for Germany, obviously, but also I'm looking forward to working with Germany. We've been discussing Germany's agenda, and your Foreign Minister was here. He spent a lot of time with the Secretary; a couple of hours in a meeting on Friday and then dinner with Secretary Rice Friday night. One of the major topics was the German agenda for its dual presidencies the first half of the year, G8 presidency for the whole year.

We've been working very closely with Germany, and we think this can really be a very successful presidency. We're very excited about this.

**Exhibit 11**

***Defendant's Motion for Partial Summary Judgment***

Source Information

Major Newspapers

**FILE-NAME:** MAJPAP

**COVERAGE:** Please see individual source records for complete coverage information

**FREQUENCY:** Varies by source, see individual source descriptions.

**HIER-LOC:**

News/Combined Sources

**CONTENT-SUMMARY:**

Access to certain freelance articles and other features within this publication (i.e. photographs, classifieds, etc...) may not be available.

United States newspapers must be listed in the top 50 circulation in Editor & Publisher Year Book. Newspapers published outside the United States must be in English language and listed as a national newspaper in Benn's World Media Directory or one of the top 5% in circulation for the country.

**COMPLETE FILE:**

The Advertiser/Sunday Mail (South Australia)  
The Arizona Republic (Phoenix)  
Arkansas Democrat-Gazette  
The Atlanta Journal and Constitution  
The Australian  
The Baltimore Sun  
The Baltimore Sun (6+ months)  
The Baltimore Sun (most recent 6 months)  
The Boston Globe  
The Boston Herald  
Brisbane News  
The Buffalo News  
Business Times (Malaysia)  
The Business Times Singapore  
The Charlotte Observer  
Chicago Sun-Times  
Chicago Tribune  
The Christian Science Monitor  
The Cincinnati Enquirer (Ohio)  
The Columbus Dispatch  
The Courier Mail/The Sunday Mail (Australia)  
The Courier-Journal (Louisville, Kentucky)  
Daily News (New York)  
The Daily/Sunday Telegraph (London)  
Daily Telegraph and Sunday Telegraph (Sydney, Australia)  
The Daily Yomiuri (Tokyo)  
The Dallas Morning News  
The Denver Post  
Detroit Free Press  
The Detroit News (Michigan)  
The Dominion Post (Wellington, New Zealand)  
The Dominion (Wellington)  
The Evening Post (Wellington)  
Financial Times (London)  
Het Financierdagblad (English)  
Fort Worth Star-Telegram  
Gazeta Mercantil Online  
The Gazette (Montreal)

The Globe and Mail (Canada)  
Grand Rapids Press (Michigan)  
The Guardian (London)  
The Hartford Courant  
The Hartford Courant (6+ months)  
The Hartford Courant (most recent 6 months)  
The Herald (Glasgow)  
Herald Sun/Sunday Herald Sun (Melbourne, Australia)  
The Houston Chronicle  
The Independent and Independent on Sunday (London)  
The Indianapolis Star (Indiana)  
The Irish Times  
The Jerusalem Post  
Journal of Commerce  
The Kansas City Star  
Los Angeles Times  
Los Angeles Times (6+ months)  
Los Angeles Times (most recent 6 months)  
The Mercury/Sunday Tasmanian (Australia)  
Miami Herald  
The Milwaukee Journal Sentinel  
New Straits Times (Malaysia)  
The New York Post  
The New York Times  
The New Zealand Herald  
Newsday (6+ months)  
Newsday (most recent 6 months)  
Newsday (New York, NY)  
The Observer  
The Oklahoman  
The Orange County Register  
The Oregonian  
Orlando Sentinel  
Ottawa Citizen  
The Philadelphia Daily News - Most Recent Two Weeks  
The Philadelphia Daily News (PA)  
The Philadelphia Inquirer  
The Philadelphia Inquirer - Most Recent Two Weeks  
Pittsburgh Post-Gazette  
The Plain Dealer  
The Press (Christchurch, New Zealand)  
Rocky Mountain News  
Sacramento Bee  
Saint Paul Pioneer Press  
San Antonio Express-News  
San Diego Union-Tribune  
The San Francisco Chronicle  
San Jose Mercury News  
The Scotsman & Scotland on Sunday  
The Seattle Times  
South China Morning Post  
St. Louis Post-Dispatch  
St. Petersburg Times  
Star Tribune (Minneapolis MN)  
The Straits Times (Singapore)  
Sun-Sentinel (Fort Lauderdale)  
The Tampa Tribune  
The Times-Picayune  
The Toronto Star  
USA Today  
The Washington Post

**Exhibit 12**

*Defendant's Motion for Partial Summary Judgment*

FOCUS™ Terms "Automated Targeting System" and date(geq (11/1/06) and leq (12/14/06)) Search Within All Documents Go FOCUS Options.

View: Cite | KWIC | Full | Custom

1-10 of 29 NEXT

FAST Print

Print | Download | Fax | Email | Text Only

Save As Alert | Hide Hits

Source: News & Business > / . . . / > Major Newspapers

Terms: "automated targeting system" and date(geq (11/1/06) and leq (12/14/06)) (Edit Search | Suggest Terms for My Search)

Select for FOCUS™ or Delivery

- 1. The Toronto Star, December 14, 2006 Thursday, NEWS; Pg. A10, 777 words, Bush faces fight on privacy rights, Tim Harper, Toronto Star, WASHINGTON  
... establishing the so-called **Automated Targeting System**, a data-mining ...
- 2. The Washington Post, December 14, 2006 Thursday, Final Edition, Financial; D04, 395 words, Air Passenger Data Program Concerns European Officials, Ellen Nakashima, Washington Post Staff Writer  
... said. At issue is the **Automated Targeting System**, a computerized screening ...
- 3. Fort Worth Star-Telegram (Texas), December 11, 2006 Monday, B; Pg. 9, 844 words, No mother lode here, JIM HARPER, The CATO INSTITUTE  
... Security put into effect the **Automated Targeting System** last week, it ...
- 4. The San Diego Union-Tribune, December 11, 2006 Monday, OPINION; Pg. B-7, 891 words, Is there a civil war in Iraq? Your call, Gina Lubrano, READERS REPRESENTATIVE  
... keyword, type in "**automated targeting system.**" Hit submit. That will ...
- 5. The Daily Telegraph (LONDON), December 9, 2006 Saturday, TRAVEL; Pg. 4, 257 words, British visitors to US given 'terror rating', Jeremy Skidmore  
... 29 to comment on the **Automated Targeting System** (ATS), dubbed the "terror ...
- 6. St. Louis Post-Dispatch (Missouri), December 9, 2006 Saturday, THIRD EDITION, EDITORIAL; Pg. A41, 821 words, Who ordered the falafel?  
... by the department's computerized **Automated Targeting System** over the last four ...
- 7. The Washington Post, December 9, 2006 Saturday, Final Edition, A Section; A02, 801 words, Traveler Data Program Defied Ban, Critics Say; Congress Barred Funds for DHS Development, Spencer S. Hsu and Ellen Nakashima, Washington Post Staff Writers  
... important elements of the controversial **Automated Targeting System** program to lawmakers in ...
- 8. The Guardian (London) - Final Edition, December 8, 2006 Friday, GUARDIAN WEEKLY; Pg. 7, 423 words, Guardian Weekly: US News: Millions assigned terror risk score on trips to America, Ed Pilkington in New York  
... details of the system, known as the **Automated Targeting System** or ATS, were put on the ...
- 9. St. Louis Post-Dispatch (Missouri), December 7, 2006 Thursday, THIRD EDITION, EDITORIAL; Pg. C11, 857 words, Data mining can't improve our security. But it does invade our privacy., By Jim Harper  
... Security put into effect its **Automated Targeting System** this week, it added to ...
- 10. Christian Science Monitor, December 6, 2006, Wednesday, USA; Pg. 3, 829 words, Furor over 'terror scores' for airline travelers, Alexandra Marks Staff writer of The Christian Science Monitor, NEW YORK  
... claiming the program - called the **Automated Targeting System** (ATS) - violates a ...

Source: News & Business > / . . . / > Major Newspapers

Terms: "automated targeting system" and date(geq (11/1/06) and leq (12/14/06)) (Edit Search | Suggest Terms for My Search)

Select for FOCUS™ or Delivery

- 11. The Columbus Dispatch (Ohio), December 6, 2006 Wednesday, Home Final Edition, EDITORIAL & COMMENT; Pg. 10A, 375 words, Keeping score; Federal program scrutinizing air travelers is useful but requires oversight  
... for mistakes or abuse, the **Automated Targeting System** should be subject to close oversight. ...
- 12. The Oregonian (Portland, Oregon), December 5, 2006 Tuesday, Sunrise Edition, Editorial; Pg. C06, 481 words, EDITORIAL - Sir, you appear to be a 25.6; please step over here, The Oregonian  
The scope of the department's expanded **Automated Targeting System** was revealed in the dry ...  
... overdue for oversight." The **Automated Targeting System** isn't new, but ...  
... see and challenge their information. The **Automated Targeting System**, according to the Associated Press, ...
- 13. Journal of Commerce, December 4, 2006 Monday, COLUMNS; Pg. 46, 769 words, Embracing '10+2', BY PETER TIRSCHWELL  
... despite Customs' assurances that its **Automated Targeting System** is still effective in ...
- 14. The Boston Herald, December 2, 2006 Saturday, ALL EDITIONS, FINANCE; Pg. 020, 359 words, THE TICKER  
... Security Department's computerized **Automated Targeting System**, or ATS. - STAFF AND WIRE ...
- 15. Chicago Tribune, December 2, 2006 Saturday, Chicago Final Edition, NEWS; ZONE C; Pg. 1, 1069 words, U.S. secretly gathers data on travelers; Privacy experts decry program, By Frank James, Washington Bureau. "Assessing risk" list by the Associated Press, WASHINGTON  
... 4-year-old **Automated Targeting System**, or ATS, aren't accessible ...  
... data used by the **Automated Targeting System** to assess international travelers' ...
- 16. The Guardian (London) - Final Edition, December 2, 2006 Saturday, GUARDIAN INTERNATIONAL PAGES; Pg. 26, 595 words, Millions assigned terror risk score on trips to the US: Information gleaned from travellers to build profiles Rights groups protest over 'decimation' of Privacy Act, Ed Pilkington, New York  
... details of the system, known as the **Automated Targeting System** or ATS, were put on the ...
- 17. The Houston Chronicle, December 2, 2006 Saturday, 3 STAR EDITION, A; Pg. 10, 358 words, Top secret traveler threat list draws fire; Senator plans to investigate a system that has no oversight, MICHAEL J. SNIFFEN, Associated Press, WASHINGTON  
... Security Department's computerized **Automated Targeting System**, or ATS. The travelers are not ...
- 18. The Irish Times, December 2, 2006 Saturday, WORLD; Pg. 13, 587 words, Millions of travellers get US terror rating, Ed Pilkington in New York  
... details of the system, known as the **Automated Targeting System** or ATS, were put on the ...
- 19. Ottawa Citizen, December 2, 2006 Saturday, Final Edition, NEWS; Pg. A3, 544 words, The perils of modern flight: Air travellers to U.S. to be given secret 'terrorism threat' rating, Tim Reid, The Times, London, WASHINGTON  
... it. The program, called the **Automated Targeting System** (ATS), was disclosed by the ...
- 20. The Philadelphia Inquirer, December 2, 2006 Saturday, NATIONAL; Pg. A04, 482 words, In the Nation  
... assessed by the computerized **Automated Targeting System**. Leahy said it was " ...

Select for FOCUS™ or Delivery

- 21. THE SAN FRANCISCO CHRONICLE (California), December 2, 2006 Saturday, FINAL Edition, EDITORIAL; LETTERS TO THE EDITOR; Pg. B6, 939 words, LETTERS TO THE EDITOR ... privacy is the secret ATS (**Automated Targeting System**) records that have been kept on ...
- 22. Sun-Sentinel (Fort Lauderdale, Florida), December 2, 2006 Saturday, Broward Metro Edition, NATIONAL; Pg. 8A, 238 words, AIR TRAVELERS OBJECT TO SECRET U.S. SCREENING, WASHINGTON {BYLINE} The Associated Press ... Security Department's computerized **Automated Targeting System**, or ATS. The travelers are not ...
- 23. The Toronto Star, December 2, 2006 Saturday, NEWS; Pg. A23, 785 words, U.S. tracks Canadians for terror traits, Tim Harper, Toronto Star, WASHINGTON ... a program known as the **Automated Targeting System** (ATS). ... trying to hide the program. "The **Automated Targeting System** mines a vast ...
- 24. The Washington Post, December 2, 2006 Saturday, Final Edition, A Section; A05, 588 words, ACLU Urges U.S. to Stop Collection of Traveler Data, Ellen Nakashima, Washington Post Staff Writer ... leaves the United States. The **Automated Targeting System** began as a means of ...
- 25. The Houston Chronicle, December 1, 2006 Friday, 3 STAR EDITION, A; Pg. 6, 364 words, Feds rate air travelers for terrorism; All international fliers, including Americans, are assessed for risk by a computer, Associated Press, WASHINGTON ... an announcement detailing the **Automated Targeting System**, or ATS, in the Federal ...
- 26. San Jose Mercury News (California), December 1, 2006 Friday, 2493 words, Additional 'Letters to the Editor' ... Homeland Security running the **automated targeting system** on travelers the Electronic ...
- 27. Sun-Sentinel (Fort Lauderdale, Florida), December 1, 2006 Friday, Broward Metro Edition, NATIONAL; Pg. 3A, 425 words, U.S. IS GIVING YOU TERROR THREAT SCORE; SECRET PROGRAM ASSESSES TRAVELERS; FILE KEPT 40 YEARS, WASHINGTON {BYLINE} By Michael J. Sniffen The Associated Press ... an announcement detailing the **Automated Targeting System**, or ATS, for the first ...
- 28. Chicago Tribune, November 3, 2006 Friday, Chicago Final Edition, NEWS ; ZONE C; ACROSS THE NATION ; Pg. 10, 189 words, U.S. plans to screen all who cross borders, Items compiled from Tribune news services., WASHINGTON, D.C. ... a program called the **Automated Targeting System**, designed to screen shipping ...
- 29. The Washington Post, November 3, 2006 Friday, Final Edition, A Section; A18, 1072 words, U.S. Plans to Screen All Who Enter, Leave Country; Personal Data Will Be Cross-Checked With Terrorism Watch Lists; Risk Profiles to Be Stored for Years, Ellen Nakashima and Spencer S. Hsu, Washington Post Staff Writers ... a program called the **Automated Targeting System**, originally designed to screen ... ... Congress has been unaware of the potential of the **Automated Targeting System** to assess non-aviation ... ... a full interview. The **Automated Targeting System** relies on government ... ... DHS notice specified that the **Automated Targeting System** does not call for ...

Source: News & Business > / ... / > Major Newspapers 

Terms: "automated targeting system" and date(geq (11/1/06) and leq (12/14/06)) (Edit Search | Suggest Terms for My Search)

View: Cite

Date/Time: Wednesday, February 21, 2007 - 11:19 AM EST



LexisNexis®

[About LexisNexis](#) | [Terms & Conditions](#)

Copyright © 2007 LexisNexis, a division of Reed Elsevier Inc. All rights reserved.

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC FRONTIER FOUNDATION )  
)  
Plaintiff, )  
)  
v. )  
)  
DEPARTMENT OF HOMELAND )  
SECURITY )  
)  
Defendant. )  
\_\_\_\_\_ )

**Consolidated Cases**  
Civil Action No. 06-1988 (ESH)  
Civil Action No. 06-2154 (RBW)

**ORDER**

UPON CONSIDERATION of plaintiff’s motion for partial summary judgment and defendant’s cross-motion for partial summary judgment on the issue of plaintiff’s entitlement to expedited processing of its requests submitted to defendant Department of Homeland Security under the Freedom of Information Act, 5 U.S.C. § 552, the parties’ opposition briefs, and the entire record, it is this \_\_\_\_ day of \_\_\_\_\_, 2007;

**ORDERED** that plaintiff’s motion is hereby denied; and it is

**FURTHER ORDERED** that defendant’s motion is hereby granted; and it is

**FURTHER ORDERED** that the parties shall appear at a status hearing on

\_\_\_\_\_ at \_\_\_\_\_ in order to establish dates for defendant’s production of responsive, non-exempt agency records.

\_\_\_\_\_  
UNITED STATES DISTRICT JUDGE