IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

PLAINTIFF'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Pursuant to Fed. R. Civ. P. 56, plaintiff Electronic Frontier Foundation respectfully moves for partial summary judgment on the issue of its entitlement to expedited processing of requests submitted to defendant Department of Homeland Security under the Freedom of Information Act, 5 U.S.C. § 552. In support of its motion, plaintiff submits the accompanying memorandum of points and authorities and statement of material facts.

Respectfully submitted,

/s/ David L. Sobel

DAVID L. SOBEL
D.C. Bar No. 360418

MARCIA HOFMANN
D.C. Bar No. 484136

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009
(202) 797-9009

Counsel for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION FOR PARTIAL SUMMARY JUDGMENT AND REQUEST FOR EXPEDITED CONSIDERATION

Plaintiff Electronic Frontier Foundation ("EFF") respectfully submits this memorandum of points and authorities in support of its motion for partial summary judgment on the issue of the expedited processing of Freedom of Information Act ("FOIA") requests pending before defendant Department of Homeland Security ("DHS"). As we explain more fully below, the FOIA requests at issue involve DHS activities that have been controversial and the subject of considerable debate because of their impact on privacy rights. The agency has acknowledged the debate that surrounds the initiatives, but has refused to grant EFF's requests for expedited processing to enable plaintiff to educate the public about these activities. Plaintiff seeks an order directing the agency to expedite the requests and, as the statute requires, process them "as soon as practicable." Given the time-sensitive nature of the statutory right at issue, plaintiff respectfully requests that the Court consider this matter expeditiously.

Statement of Facts

These consolidated cases arise from defendant DHS's handling of three FOIA requests submitted by plaintiff EFF seeking the disclosure of agency records relating to two controversial initiatives that have been the focus of substantial public interest: the U.S. government's negotiations with the European Union concerning the transfer of airline passenger data; and a large border-control data-mining operation called the Automated Targeting System ("ATS"). Plaintiff asserted a statutory right to "expedited processing" of the three requests on the ground that 1) the requests were made by "a person primarily engaged in disseminating information;" and 2) there is an "urgency to inform the public" about the subjects of the requests, 5 U.S.C. § 552(a)(6)(E)(v)(II). Defendant DHS refused to expedite the processing of the requests, finding that EFF is not "primarily engaged in disseminating information," and that there is no "urgency to inform the public."

A. Passenger Data Agreements Between the United States and European Union and the Automated Targeting System

In 2004, the United States ("U.S.") and the European Union ("EU") reached an agreement on the processing and transfer of Passenger Name Record ("PNR") data to DHS concerning flights between the U.S. and the EU.[1] Shortly thereafter, DHS issued the "Undertakings," a set of representations reflecting how DHS (specifically, Customs and Border Protection) would collect, maintain, and secure the passenger data.[2] The agreement was met with widespread

[1] 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 (May 20, 2004), http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf.

[2] The representations (formally known as the Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data) are available at 69 Fed. Reg. 41543-41547 (July 9, 2004).

international criticism centered around the issue of whether the U.S. would handle the passenger data adequately under EU privacy law.[3] The European Court of Justice ruled the U.S.-EU agreement illegal under EU law in May 2006, ordering that it become void on September 30, 2006.[4] In light of the decision, the U.S. and the EU worked to renegotiate the terms of the agreement.

In October 2006, the U.S. and the EU reached a temporary agreement on the processing and transfer of PNR data to DHS from commercial airline flights between the U.S. and the EU.[5] This understanding replaced the agreement that was reached in 2004 and subsequently found invalid by the European Court of Justice. At the time the new agreement was reached, DHS sent a letter to EU officials stating that it would more broadly construe representations the agency had made in the Undertakings about how it would handle passenger data transferred between the EU and the U.S.[6] Specifically, DHS intended to permit, among other things, more substantial

---

[3] *See, e.g.*, Denis Staunton and Sorcha Crowley, *Civil Liberties Groups Critical of Data Deal on Flights to US*, Irish Times (Ir.), Feb. 21, 2003; Press Release, European Parliament, Parliament Defends Data Protection Rights, March 13, 2003; Andrew Orlowski, *Europe Rebuffs US Flight Info Data Grab*, The Register (UK), April 1, 2004; Sara Kehaulani Goo, *Europeans Seek Court Review of Data-Sharing Plan*, Washington Post, April 22, 2004; Nicola Smith, *MEPs Reject New Vote on EU-US Air Data Deal*, TheParliament.com (Brussels), May 4, 2004; John Lettice, *Ministers Thwart MPs, OK EU-US Airline Data Deal*, The Register (UK), May 18, 2004.

[4] 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).

[5] 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, Bureau of Customs and Border Protection (Oct. 27, 2006), http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf.

[6] Letter to the Council Presidency and the Commission from the Department of Homeland Security of the United States of America, Concerning the Interpretation of Certain Provisions of the Undertakings Issued by DHS on 11 May 2004 in Collection with the Transfer by Air Carriers of Passenger Name Record (PNR) Data (Oct. 27, 2006), http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_letter_DHS_en.pdf.

disclosure of passenger data to other U.S. agencies with counterterrorism functions. The media reported extensively on the finalization of the temporary agreement and DHS's change in policy on how it would handle the EU-U.S. PNR data.[7]

On November 2, 2006, defendant DHS and its component, Customs and Border Protection, published a Federal Register notice describing a "system of records" called the "Automated Targeting System" ("ATS"). 71 Fed. Reg. 64543-64546. The ATS, as described by DHS, is a data-mining system that the agency uses to create "risk assessments" for tens of millions of travelers, including international travelers and U.S. citizens, based on extensive personal information. *Id*. at 64544. The personal data used by ATS to make determinations about travelers includes, *inter alia*, PNR data such as the records covered by the 2004 Undertakings. *Id*. at 64543.

B. Plaintiff's FOIA Request for Records Concerning the U.S.-EU Negotiations

By letter transmitted to DHS on October 20, 2006 (attached hereto as Exhibit A), plaintiff requested under the FOIA agency records concerning the renegotiated agreement between the U.S. and the EU, and the handling of PNR data under the 2004 Undertakings. Specifically, plaintiff requested the following agency records (created between May 30, 2006 and the date of the request):

> 1) emails, letters, reports, or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the U.S. for prescreening purposes;
>
> 2) emails, letters, statements, memoranda, or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the Undertakings;

[7] *See*, *e.g.*, Reuters, *U.S., Europe Reach Deal on Air Passenger Data*, Oct. 6, 2006; Associated Press, *Deal Reached on Passenger Data*, Oct. 6, 2006; Mark John, *U.S. to Seek More Leeway on Air Passenger Records*, Reuters, Oct. 17, 2006.

> 3) records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used, disclosed to other entities, or combined with information from other sources; and
>
> 4) complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data of EU citizens.

Exhibit A at 2.

Plaintiff requested expedited processing of the FOIA request under DHS's regulations, 6 CFR § 5.5(d)(1)(ii), on the ground that the request pertained to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity," and the request was made by "a person primarily engaged in disseminating information." Plaintiff provided substantial evidence that it is "primarily engaged in disseminating information" and noted that it was relying upon the same evidence in support of both its "primarily engaged" claim and its asserted entitlement to classification as a "representative of the news media" for assessment of processing fees under the FOIA and 6 C.F.R. § 5.11(b)(6).[8] *Id.* at 3. Plaintiff provided defendant DHS the following information concerning its dissemination activities in support of its claims:

> EFF is a non-profit public interest organization that works "to protect and enhance our core civil liberties in the digital age." One of EFF's primary objectives is "to educate the press, policymakers and the general public about online civil liberties." To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

[8] Subsequent to the initiation of Civil Action No. 06-1988, defendant indicated that it has reversed its earlier determination of EFF's fee status and "has granted plaintiff's request for treatment as a 'news media requester.'" Defendant's Answer to Plaintiff's Amended Complaint (C.A. No. 06-1988), ¶ 26. As a result, the parties are negotiating a stipulation that will remove plaintiff's "news media" claims from this action. The administrative record with respect to those claims remains relevant, however, because plaintiff consistently maintained that it was relying upon the same facts in support of its entitlement to both favored fee status and expedited processing.

> First, EFF maintains a frequently visited web site, http://www.eff.org, which received 40,681,430 hits in September 2006 — an average of 56,501 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.
>
> EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 77,000 subscribers. A complete archive of past EFFectors is available at http://www.eff.org/effector/.
>
> Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (http://www.eff.org/deeplinks/) reports and analyzes newsworthy developments in technology. It also provides miniLinks, which direct readers to other news articles and commentary on these issues. DeepLinks had 538,297 hits in September 2006.
>
> In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than eighteen white papers published since 2002. These papers, available at http://www.eff.org/wp/, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.
>
> EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (http://www.powells.com). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (http://www.amazon.com). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at http://cryptome.org/cracking-des.htm and for sale at Amazon.com.
>
> Most recently, EFF has begun broadcasting podcasts of interviews with EFF staff and outside experts. *Line Noise* is a five-minute audio broadcast on EFF's current work, pending legislation, and technology-related issues. A listing of *Line Noise* podcasts is available at feed://www.eff.org/rss/linenoisemp3.xml and feed://www.eff.org/rss/linenoiseogg.xml. These podcasts were downloaded more than 1,300 times from EFF's web site last month.

Id. at 3-4 (footnotes omitted).

In support of its assertion that there is an "urgency to inform the public" about the requested information, plaintiff noted that the agreement will have to be renegotiated before it

expires in July 2007 and cited the controversy surrounding the temporary agreement (and the substantial news media coverage addressing it):

> The temporary agreement on transfer of passenger data expires on July 31, 2007, and will need to be renegotiated prior to that date. The government activity at issue here — DHS's reinterpretation of privacy commitments to the EU — raises serious questions about how DHS will implement privacy safeguards and address the privacy concerns that caused controversy even under the more protective 2004 agreement. Thus, there is a particular urgency for the public to obtain information about DHS's construction of the Undertakings under the new agreement, as well as the effectiveness of the measures in place to secure passengers' data privacy. According to the Associated Press, the "arduous" negotiations to reach the interim agreement "reflected deep divisions between the United States and the European Union over anti-terror measures and to what length governments should go in curbing personal freedoms to prevent attacks." Associated Press, *Deal Reached on Passenger Data*, Oct. 6, 2006. As Reuters noted:
>
> > EU lawmakers raised worries that Washington was riding roughshod over data protection concerns in its quest after the 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.
>
> Reuters, *US., Europe Reach Deal on Air Passenger Data*, Oct. 6, 2006. These issues have attracted substantial media interest in recent days. In fact, Google News search for "privacy and 'passenger data'" returns about 621 results from news outlets throughout the world (see first page of Google News search results attached).
>
> The purpose of this request is to obtain information directly relevant to DHS's guidelines on the handling of EU-US passenger data before July 31, 2007, when the temporary agreement is set to expire. The records requested involve the manner in which DHS is construing its policies on this matter, and clearly meet the standard for expedited processing. There is clearly "an urgency to inform the public" about the Department's policies with respect to this issue in order to facilitate a full and informed public debate on the U.S. position in the upcoming bi-lateral negotiations.

Id. at 2-3.

By letter dated November 1, 2006 (attached hereto as Exhibit B), DHS denied plaintiff's request for expedited processing, asserting 1) that EFF is "not primarily engaged in the disseminating of information to the public," and 2) that EFF has not "detailed with specificity

why . . . there is an urgency to inform the public" about the Department's negotiations with the European Union with respect to the transfer of airline passenger data. The agency also denied EFF's request to be treated as a "news media" requester for purposes of fee assessments. *Id.* at 1.

Plaintiff appealed the agency's adverse determinations by letter transmitted to defendant on November 21, 2006 (attached hereto as Exhibit C). Challenging both the denial of "news media" status and agency's assertion that EFF is not "primarily engaged in disseminating information," plaintiff's counsel wrote:

> In our request letter of October 20, 2006, we provided extensive information in support of EFF's entitlement to "news media" status for purposes of fee assessments. That letter is incorporated herein by reference. In order to update the information we previously submitted, I am attaching hereto a copy of EFF's most recent newsletter, which includes coverage and analysis of issues such as electronic voting problems in the recent mid-term election, new developments in intellectual property law, a Federal Register notice published by DHS, and legislative and judicial consideration of the National Security Agency's surveillance program. I also note that since the newsletter was published last week, EFF's news blog (www.eff.org/deeplinks/) has covered additional news items, including a decision issued yesterday by the California Supreme Court concerning liability for information posted on the Internet. It is clear that this material, which EFF publishes on a regular and continuous basis, constitutes "news" within the meaning of the agency's regulations. 6 C.F.R. § 5.11(b)(6) ("The term 'news' means information that is about current events or that would be of current interest to the public."). EFF's publication of this material, *inter alia*, clearly qualifies it for classification as a "news media" entity within the meaning of the regulations. *Id.* ("Examples of news media entities include . . . publishers of periodicals . . . who make their products available for purchase or subscription by the general public.").

Id. at 1-2.[9]

On the issue of an "urgency to inform the public" about the bi-lateral passenger data negotiations, plaintiff noted in its appeal that Homeland Security Secretary Michael Chertoff had

[9] Plaintiff's counsel noted that "[w]ith respect to the dissemination issue, I incorporate by reference the information we have provided with respect to EFF's entitlement to 'news media' status." *Id.* at 2.

recently underscored both the importance of, and the debate surrounding, the international exchange of passenger data:

> As for the "urgency" issue, [the agency] asserted that EFF has not "offer[ed] any evidence of public interest that is greater than the public's general interest in the transfer and use of passenger name data." In appealing from that determination, I reiterate and incorporate the information initially provided to the agency in support of EFF's FOIA request. In addition, and to update the relevant "evidence," I note that Secretary Chertoff delivered a speech to the Federalist Society on November 17, in which he saw fit to highlight the dispute between the United States and the EU on passenger data. *See* http://www.dhs.gov/xnews/speeches/sp_1163798467437.shtm. The full text of that speech is incorporated herein by reference, and I specifically note the Secretary's acknowledgement that the privacy issues surrounding the transfer of passenger data "led to a very substantial debate." *See also* Reuters, "Chertoff says U.S. threatened by international law," November 17, 2006 (attached hereto). It is precisely the "substantial debate" the Secretary noted that establishes the public interest in the requested material. EFF is clearly entitled to the expedited processing of its request.

Id. at 2.[10]

Plaintiff filed suit upon the agency's failure to respond to plaintiff's request for records within the 20-working-day period set forth in the FOIA, 5 U.S.C. § 552(a)(6)(A). After DHS failed to timely respond to EFF's administrative appeal, plaintiff amended its complaint on December 21, 2006, to allege, *inter alia*, that defendant had unlawfully denied plaintiff's request for expedited processing.

C. Plaintiff's FOIA Requests for Records Concerning the Automated Targeting System

By letters to DHS dated November 7, 2006, and December 6, 2006 (attached hereto as Exhibits E & F), plaintiff requested information concerning the Automated Targeting System. In its November 7 request, plaintiff requested the following agency records:

[10] For the Court's convenience, the text of Secretary Chertoff's speech to the Federalist Society is attached hereto as Exhibit D.

> 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 ("CPB") and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information; and
>
> 3) all records, including Privacy Act notices, that discuss or describe the use of personally-identifiable information by CPB (or its predecessors) for purposes of "screening" air and sea travelers.

Exhibit E at 1.[11] In its December 6 letter, plaintiff requested additional records concerning the ATS relating to claims made by DHS officials in defense of the system and criticisms of the system raised in public comments submitted in response to the agency's Federal Register notice. Exhibit F.

Plaintiff requested expedited processing of both FOIA requests, stating that they meet the criteria for expedited processing under defendant DHS's regulations, 6 C.F.R. § 5.5(d)(1)(ii), because they pertain to a matter about which there is an "urgency to inform the public," and the requests are made by "a person primarily engaged in disseminating information." Exhibit E at 2; Exhibit F at 3. In both requests, plaintiff provided defendant DHS with the same evidence demonstrating that EFF is "primarily engaged in disseminating information" as plaintiff had provided in its FOIA request concerning the U.S.-EU passenger data negotiations. *Compare* Exhibits E & F *with* Exhibit A.

In its letter of November 7, 2006, plaintiff supported its assertion that there is an "urgency to inform the public" about the ATS by noting that there had already (just a few days after the publication of the DHS Federal Register notice) been significant news media attention devoted to

[11] To assist the agency in searching for records responsive to the third item in its request, plaintiff noted that an Associated Press article dated November 3 (and attached to the request letter) quoted DHS spokesman Russ Knocke as saying that "screening for air and sea travelers has been in place since the 1990s."

the system. Exhibit E at 2. Plaintiff also asserted that the agency's solicitation of public comments created a compelling need for expeditious disclosure.

> First, there is substantial public interest in the Department's use of the ATS to assign "risk assessments" to American citizens. A search conducted on Google News indicates that since the Federal Register notice was published five days ago, 58 articles have been published that discuss the system and the privacy issues it raises (see first page of search results, attached hereto). The published articles include coverage by the Washington Post and the Associated Press (see attached articles).
>
> Further, there is an "urgency to inform the public" about the potential privacy implications of the ATS because the Department has solicited public comments and announced that "[t]he new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination." 71 FR 64543. Indeed, it is difficult to imagine circumstances where there would be a greater "urgency to inform the public" than when an agency has solicited public comment on a significant issue, set a short deadline for the submission of comments, and stated its intention to go forward with its proposal "unless comments are received that result in a contrary determination."
>
> The purpose of this request is to obtain information directly relevant to DHS's Privacy Act notice and the practices it describes (which will affect tens of millions of American citizens). 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 on the issue prior to the December 4 deadline the Department has imposed.

Id.

In its letter of December 6, 2006, plaintiff noted the extraordinary news media interest in the ATS that had occurred in a little more than a month since the publication of the Federal Register notice (which confirmed plaintiff's earlier assertion of public interest). Exhibit F at 3. Plaintiff also noted that leading members of Congress had expressed concerns about the privacy implications of the system and announced legislative consideration of the issue:

> [T]here is substantial public interest in the Department's use of the ATS to assign "risk assessments" to American citizens. A search conducted on Google News indicates that since the Federal Register notice was published on November 2, almost 900 articles have been published that discuss the system and the privacy issues it raises (see first page of search results, attached hereto as Exhibit 2). The

> published articles include coverage by the Washington Post and the Associated Press (see Exhibits 3 & 4).
>
> Further, there is an "urgency to inform the public" about the potential privacy implications of the ATS because the Department has solicited public comments and yesterday extended the comment period until December 29. In addition, Sen. Patrick Leahy, incoming chairman of the Senate Judiciary Committee, has announced that oversight of the ATS and similar systems will occur when the new Congress convenes in January. Exhibits 1 & 5. Similarly, Senate Homeland Security Investigations Subcommittee Chairman Norm Coleman has indicated he also is examining the system. Sen. Coleman said, "We must ensure that this program is indeed working to prevent terrorism, while at the same time safeguarding the privacy of air travelers." Exhibit 1. Rep. Bennie Thompson, incoming chairman of the House Homeland Security Committee has written in a letter to Secretary Chertoff that "serious concerns have arisen that . . . some elements of ATS as practiced may constitute violations of privacy or civil rights." Exhibit 6.
>
> The purpose of this request is to obtain information directly relevant to DHS's Privacy Act notice and the practices it describes (which will affect tens of millions of American citizens). 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, and prior to the Congressional consideration of the system when the new Congress convenes in January.

Id. at 3-4.

By letter to plaintiff dated December 14, 2006 (attached hereto as Exhibit G), DHS advised plaintiff that the agency had "aggregated" plaintiff's FOIA requests dated November 7, 2006, and December 6, 2006, "to simplify processing." Exhibit G at 1. Defendant further advised plaintiff that "[a]s it relates to your request for expedited treatment, your request is denied," because "you are not primarily engaged in the disseminating of information to the public," and "[you have not] detailed with specificity why you feel there is an urgency to inform the public about this topic." *Id.* at 3. Plaintiff filed suit on December 19, 2006, alleging that DHS has violated the FOIA with respect to the expedited processing of these requests.

On January 31, 2007, the Court consolidated these cases "for the purpose of deciding plaintiff's request[s] for expedited processing under FOIA." Minute Order, January 31, 2007. Plaintiff now moves for partial summary judgment on the issue of expedited processing.

ARGUMENT

The issues raised in this motion are straightforward and not subject to serious dispute. In compliance with the FOIA and applicable DHS regulations, plaintiff requested expedited processing of requests seeking information concerning the U.S.-EU passenger data negotiations and the Automated Targeting System. In support of its requests, plaintiff submitted specific and relevant information that clearly established its entitlement to expedited processing. In violation of the statutory and regulatory requirements for expedited processing, defendant DHS denied plaintiff's requests. The agency's action is clearly unlawful and should be enjoined.

I. The Court has Jurisdiction to Grant the Requested Relief

The Court's jurisdiction to consider this matter and grant appropriate relief is clear. The FOIA provides, in pertinent part:

> Agency action to deny or affirm denial of a request for expedited processing . . . shall be subject to judicial review under paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

5 U.S.C. § 552(a)(6)(E)(iii). The referenced judicial review provision states, in pertinent part:

> On complaint, the district court of the United States . . . in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo . . . .

5 U.S.C. § 552(a)(4)(B). *See Al-Fayed v. CIA*, 254 F.3d 300, 304 (D.C. Cir. 2001).[12]

[12] Plaintiff filed an administrative appeal of the agency's denial of expedited processing with respect to the U.S.-EU agreement, but did not file an appeal of the agency's denial with respect to the ATS request. Both of plaintiff's claims are nonetheless ripe for adjudication, as all

As the FOIA provides, in reviewing defendant's actions, "the court shall determine the matter *de novo*." 5 U.S.C. § 552(a)(4)(B); *see also Al-Fayed*, 254 F.3d at 308 ("[A] district court must review *de novo* an agency's denial of a request for expedition under FOIA.").

II. Plaintiff is Entitled to Expedited Processing of its FOIA Requests

The administrative record shows that plaintiff established beyond any question that its FOIA requests satisfy the statutory and regulatory requirements for expedited processing. Upon *de novo* review, the Court should enter judgment for plaintiff on the expedition issue and order defendant DHS to process plaintiff's requests as soon as practicable.

A. The Statutory and Regulatory Framework

In 1996, Congress passed the Electronic Freedom of Information Act Amendments, which, *inter alia*, added to FOIA a requirement that agencies provide for expedited processing of requests when "the person requesting the records demonstrates a compelling need." 5 U.S.C. § 552(a)(6)(E)(i). The statute defines "compelling need" to include "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). When expedition is appropriate, an agency is obligated to process the request "as soon as practicable." *Id.* § 552(a)(6)(E)(iii).

In conformance with the statute, defendant DHS promulgated a regulation providing, in pertinent part, that "[r]equests . . . will be taken out of order and given expedited treatment

---

applicable administrative remedies have been exhausted. This Court has expressly held that a party requesting expedition under FOIA may seek judicial review of an agency denial of expedition without first submitting an administrative appeal of such denial. *See, e.g.*, *American Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24, 28-29 (D.D.C. 2004) (administrative appeal is not a "prerequisite for judicial review," thus "plaintiffs' failure to appeal the FBI's refusal to expedite their request does not preclude judicial review of the decision") (emphasis omitted); *Elec. Privacy Info. Ctr. v. Dep't of Defense*, 355 F. Supp. 2d 98, 100 n.1 (D.D.C. 2004) (same).

whenever it is determined that they involve . . . [a]n urgency to inform the public about an actual or alleged federal government activity, if made by a person primarily engaged in disseminating information." 6 CFR § 5.5(d)(1). "If a request for expedited treatment is granted, the request shall be given priority and shall be processed as soon as practicable." *Id.* § 5.5(d)(4).

B. EFF is "Primarily Engaged in Disseminating Information"

Defendant DHS denied all three of plaintiff's requests for expedited processing at issue here on the ground that EFF is not "primarily engaged in disseminating information." As the record shows, plaintiff presented ample evidence of its longstanding, varied and comprehensive dissemination of information to the public. Having conceded that EFF *is* entitled to treatment as a "news media" requester for fee assessment purposes based upon its information dissemination activities, the agency must now justify its incongruous determination that the organization is somehow categorically disqualified from obtaining expedited processing of its FOIA requests. The agency's position contradicts the clear precedent of this Court, and runs counter to the express policy of other federal agencies. The position is absurd and cannot be sustained.

1. This Court has Held that "News Media" Requesters Satisfy the "Dissemination" Prong of the Expedition Standard

This Court has already rejected the scenario that defendant's administrative rulings create: a FOIA requester deemed to be a "representative of the news media" for fee purposes under 5 U.S.C. § 552(a)(4)(A)(ii), on the one hand, but simultaneously deemed *not* to be "primarily engaged in disseminating information" for expedition purposes under 5 U.S.C. § 552(a)(6)(E)(v). In *American Civil Liberties Union v. Dep't of Justice*, 321 F. Supp. 2d 24 (D.D.C. 2004) ("*ACLU*"), the Court considered the status of the Electronic Privacy Information Center ("EPIC"), which in earlier litigation had been found to qualify for "news media" treatment. *See Elec. Privacy Info. Ctr. v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

Relying upon the organization's settled status as a "news media" entity, the Court "conclude[d] that EPIC is indeed 'primarily engaged in disseminating information' for the purposes of expediting the request." 321 F. Supp. 2d at 29 n.5 (citation omitted). That conclusion is mandated by both logic and obvious congressional intent.

The rationales behind preferred fee status for "news media" requesters and expedited processing for those "primarily engaged in disseminating information" are the same – favoring those uses of the FOIA that result in the widest possible distribution of government information. It is clear that Congress anticipated that entities qualifying for preferred "news media" fee status under FOIA would be those that are "primarily engaged in disseminating information." Indeed, the legislative history of the 1986 FOIA amendments, which established preferential fee treatment for "news media" requesters, emphasized that dissemination of information was an essential requirement for the favored status. As the D.C. Circuit has noted,

> because one of the purposes of [the 1986 amendments] is to encourage the dissemination of information in Government files, as Senator Leahy (a sponsor) said: "It is critical that the phrase 'representative of the news media' be broadly interpreted if the act is to work as expected. . . . In fact, *any person or organization which regularly publishes or disseminates information to the public . . . should qualify for waivers as a 'representative of the news media.*'" 132 Cong. Rec. S14298 (daily ed. Sept. 30, 1986) (emphasis added). Representatives English and Kindness echoed Senator Leahy's sentiments: "A request by a reporter or other person affiliated with a newspaper, magazine, television or radio station, *or other entity that is in the business of publishing or otherwise disseminating information to the public* qualifies under this provision." 132 Cong. Rec. H9463 (Oct. 8, 1986) (emphasis added).

National Security Archive v. Dep't of Defense, 880 F.2d 1381, 1386 (D.C. Cir. 1989), *cert. denied*, 494 U.S. 1029 (1990) (emphasis in original). There can be no doubt that this Court's prior holding on the issue is correct – an entity that qualifies for "news media" fee status is likewise eligible for expedited processing of its requests when there is an "urgency to inform the public."

2. Many Agencies Expressly Recognize that "News Media" Requesters Satisfy the "Dissemination" Test for Expedition

Contrary to the position that defendant DHS has adopted here, many federal agencies have promulgated regulations expressly recognizing that entities qualifying for "news media" fee treatment should be deemed to be "primarily engaged in disseminating information" for purposes of expedited processing. Thus, the Department of Defense FOIA regulations provide as follows:

> Compelling need . . . means that the information is urgently needed by an individual primarily engaged in disseminating information in order to inform the public concerning actual or alleged Federal Government activity. An individual primarily engaged in disseminating information means a person whose primary activity involves publishing or otherwise disseminating information to the public. *Representatives of the news media would normally qualify as individuals primarily engaged in disseminating information*. Other persons must demonstrate that their primary activity involves publishing or otherwise disseminating information to the public.

32 CFR § 286.4(d)(3)(ii) (emphasis added), citing *id*. § 286.28(e) (fee assessment regulation); *see also* 32 CFR 518.8(d)(2)(ii) (Army regulation with identical language), 32 CFR § 701.8 (f)(5)(ii) (Navy regulation with identical language). Other agencies, including the Department of Agriculture (7 CFR § 1.9(b)(2)), Department of the Interior (43 CFR § 2.14(a)(2)), and the Social Security Administration (20 CFR § 402.140(d)), recognize that "news media" requesters are "primarily engaged in disseminating information" under the standards governing expedited processing.[13]

[13] Defendant DHS's regulations acknowledge the close relationship of the two categories, albeit not quite as explicitly as the regulations cited above. The DHS regulations provide that a requester claiming entitlement to expedition under 6 CFR § 5.5(d)(1)(ii) "if 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." 6 CFR § 5.5(d)(3). The regulation suggests that a requester such as EFF – having satisfied the agency's criteria for "news media" status – should not be required to "establish" anything further with respect to information dissemination.

To the extent that defendant DHS purports to hold "news media" requesters seeking expedition to a different standard than do other federal agencies, the DHS approach must be rejected. Noting that the statute "sets a government-wide rather than agency-specific standard" for expedited processing, the D.C. Circuit has recognized the importance of consistency in the application of FOIA's expedition provision, *Al-Fayed*, 254 F.3d at 307. The odd interpretation of the statute that DHS appears to have adopted cannot be sustained.[14]

C. Plaintiff's FOIA Requests Satisfy the "Urgency to Inform the Public" Standard

Defendant DHS erroneously maintains that plaintiff has failed to show that there is an "urgency to inform the public" about the passenger data negotiations and the Automated Targeting System. The court of appeals has held that

> in determining whether requestors have demonstrated "urgency to inform," and hence "compelling need," courts must consider at least three factors: (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.

[14] Defendant DHS has never articulated its rationale for simultaneously concluding that EFF qualifies as a "news media" entity for fee purposes, but that it does *not* qualify as being "primarily engaged in disseminating information" for expedition purposes. It is thus unclear what criteria the agency applies to distinguish between 1) dissemination activities that are adequate for favorable fee treatment but *not* adequate for expedition; and 2) dissemination activities that are adequate for *both* purposes. In any event, it is clear that EFF qualifies as an entity "primarily engaged in disseminating information" even in the absence of its conceded "news media" status. In the only opinion of which plaintiff is aware that considers the "primarily engaged" standard independent of the "news media" standard, this Court found that the Leadership Conference on Civil Rights is "primarily engaged in disseminating information" based upon some of the same kinds of activities EFF relies upon here. *See Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) ("serve[s] as the site of record for relevant and up-to-the minute civil rights news and information;" and "disseminates information regarding civil rights and voting rights to educate the public, promote effective civil rights laws, and ensure their enforcement"). Indeed, EFF relies upon a showing of far more information dissemination than was found adequate in *Leaderhip Conference*.

Al-Fayed, 254 F.3d at 310. In *ACLU*, this Court applied those factors in circumstances similar to those present here, and found that a FOIA request that "implicate[d] important individual liberties and privacy concerns . . . of immediate public interest in view of [an] ongoing [policy] debate," 321 F. Supp. 2d at 29, satisfied the "urgency to inform" standard and required expedited processing. As the Court recently noted, "judges of this Court have found sufficient exigency to grant expedited processing in situations where there was an ongoing public controversy associated with a specific time frame." *Long v. Dep't of Homeland Security*, 436 F. Supp. 2d 38 (D.D.C. 2006), citing *Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); and *ACLU*. *See also Gerstein v. CIA*, 2006 U.S. Dist. LEXIS 89847, *19 (D. Cal. November 29, 2006) (expedition required where FOIA request sought records on issue that was "subject of an ongoing national debate at the time" the request was made). Application of the relevant factors here establishes that plaintiff has shown an "urgency to inform the public" with respect to its requests.

1. <u>The Passenger Data Negotiations Request</u>

In its October 20, 2006, letter to defendant DHS, plaintiff noted that the temporary U.S.-EU agreement on the transfer of passenger data "expires on July 31, 2007" and that '[t]he government activity at issue here – DHS's reinterpretation of privacy commitments to the EU – raises serious questions about how DHS will implement privacy safeguards and address the privacy concerns that [have] caused controversy." Exhibit A at 2. Plaintiff further noted that the issue had "attracted substantial media interest in recent days," and quoted an Associated Press article reporting that the "arduous" negotiations "reflected deep divisions between the United States and the European Union over anti-terror measures and to what length governments should go in curbing personal freedoms to prevent attacks." *Id*. Noting that "[t]he purpose of this

request is to obtain information directly relevant to DHS's guidelines on the handling of EU-U.S. passenger data before July 31, 2007, when the temporary agreement is set to expire," plaintiff asserted that "[t]here is clearly 'an urgency to inform the public' about the Department's policies with respect to [the privacy of passenger data] in order to facilitate a full and informed public debate on the U.S. position in the upcoming bi-lateral negotiations." *Id*.

On November 17, 2006 – just two weeks after the agency issued its initial determination denying EFF's request for expedition – Homeland Security Secretary Chertoff, acknowledging the media coverage of the issue, highlighted the controversy surrounding passenger data in a speech to the Federalist Society: "Some of you may have followed in the press that there was a difference of opinion between the European Union and the United States about the use of something called passenger name record data . . . ." Exhibit D. He went on to note the "very substantial debate" on what he described as a "fundamental" issue:

> [P]rivacy advocates, particularly in the European Parliament believe that because that information is collected in, among other places, Europe, they should determine how we use that information in deciding who is going to be allowed into our country. *And this led to a very substantial debate*. Fortunately, we resolved it with an agreement which I think does address the principal concerns that we have. But it focused my attention on how much of my ability to do my job in leading a department that protects the American people depends upon constraints that others want to put upon us based on their conception of either international law or transnational law. *So I've come to see in a very dramatic way, this has a real world impact on the fundamental issues about how we protect ourselves*.

Id. (emphasis added).

This case is similar to the circumstances in *ACLU*, where 1) controversial provisions of the Patriot Act were set to expire; 2) the issue had attracted significant news coverage; and 3) plaintiffs sought the expedited disclosure of information for "the ongoing national debate about whether Congress should renew . . . [the] provisions before they expire." 321 F. Supp. 2d at 30.

The "host of factors" plaintiff relies upon here likewise satisfies the "urgency to inform" requirement. *Id.* at 31; *see also Leadership Conference*, 404 F. Supp. 2d at 260 (citing "upcoming expiration" of legislation; fact that disclosure could have a "a vital impact" on public debate; and presence of relevant "news reports and magazine articles" in the record).

2. The Automated Targeting System Requests

In its November 7, 2006, letter to defendant DHS, plaintiff noted that there had already been significant news media attention devoted to the ATS in the five days since the agency had published its Federal Register notice describing its use of the system to assign "risk assessment" scores to tens of millions of travelers. Exhibit E at 2 (citing 58 articles listed in a Google News search, including coverage by the Washington Post and the Associated Press). Plaintiff also asserted that the agency's solicitation of public comments on the system (with a 30-day deadline) created a compelling need for expeditious disclosure. *Id.*

Plaintiff's assertion of public interest in the ATS was dramatically proven correct as the deadline for public comments approached and the controversial DHS initiative generated a storm of media coverage and strong public and congressional criticism. In its December 6, 2006, letter to defendant DHS, plaintiff noted that a more recent search conducted on Google News "indicates that since the Federal Register notice was published on November 2, almost 900 articles have been published that discuss the system and the privacy issues it raises." Exhibit F at 3. Plaintiff further noted that the agency had extended the public comment period until December 29, and that "oversight of the ATS and similar systems will occur when the new Congress convenes in January." *Id.* Plaintiff attached to its letter a statement on the ATS by Sen. Patrick Leahy, then-incoming Chairman of the Senate Judiciary Committee, and several

news articles describing the "public outcry," "outrage," and "serious concerns" that disclosure of the plans for the ATS had generated. *See id.*

Unbeknown to plaintiff at the time it submitted its second request to defendant DHS, the agency had already embarked upon a public relations campaign to counter the media attention and criticism that the Federal Register notice had attracted. On December 4, 2006, an agency "Policy Advisor" circulated an e-mail message titled "ATS Talking Points and Background." It noted that "[l]ast Friday, several media outlets were reporting on CBP's Automated Targeting System (ATS) System of Records Notice (SORN) that was published in the Federal Register." Exhibit H.[15] It advised recipients that "[i]n an effort to prepare you for any questions you might receive on the program, please find attached the DHS Talking Points on the issue and a background paper by CBP on the issue." *Id.* It is thus clear that, notwithstanding its denial of plaintiff's request for expedited processing, the agency recognized the emerging public debate on the issue and sought to influence public opinion on the controversial system.

The "ongoing national debate" on the ATS, as in *ACLU* and *Leadership Conference*, warrants the expedited processing of information that is likely to contribute to public and congressional consideration of the issue. Given the DHS "talking points" and the agency's own public relations efforts in support of the system, expedition is particularly important, because "a meaningful and truly democratic debate . . . cannot be based solely upon information that the

[15] The e-mail message and attached "Automated Targeting System Talking Points" were recently released to plaintiff by defendant DHS in what the agency described as it "first partial release to your Freedom of Information Act request." The agency represented that the material was located in the DHS Office of Policy, and that the agency continues to process the request with respect to seven other agency components.

Administration voluntarily chooses to disseminate." *Elec. Privacy Info. Ctr. v. DOJ*, 416 F. Supp. 2d 30, 41 n.9 (D.D.C. 2006) (citation and quotations omitted).[16]

D. The Court Should Order Defendant DHS to Complete the Processing of Plaintiff's FOIA Requests "As Soon As Practicable"

As we have shown, plaintiff is "primarily engaged in disseminating information," and it demonstrated that there is an "urgency to inform the public" about the privacy implications of the U.S.-EU passenger data negotiations and the Automated Targeting System. As such, plaintiff is legally entitled to the expedited processing of its requests and the agency is required to process the requests "as soon as practicable." 5 U.S.C. § 552(a)(6)(E)(iii). As the Court did in *ACLU*, 321 F. Supp. 2d at 38, it should schedule a status hearing within ten days of its decision on this motion "in order to establish dates for the defendant's production of responsive documents." *See also EPIC v. DOJ*, 416 F. Supp. 2d at 43 (agency ordered to "complete the processing of [plaintiff's] FOIA requests and produce or identify all responsive records within 20 days").

III. The Court Should Expedite its Consideration of this Matter

As noted, *supra* n.16, the refusal of defendant DHS to expedite the processing of plaintiff's FOIA requests has already hampered the ability of plaintiff, and the public generally, to participate fully in important policy debates involving significant privacy issues. But those debates are ongoing and can still benefit from the expedited disclosure of relevant agency

[16] To some extent, the public debate on the ATS has already suffered from the agency's refusal to expedite the processing of relevant information. As noted, defendant DHS extended the public comment period on its Federal Register notice until December 29, 2006, but that deadline passed without the disclosure of the requested information. The propriety of the agency's denial of expedition, however, must be assessed based upon the circumstances that existed at the time it rendered its decision. *See* 5 U.S.C. § 552(a)(6)(E)(iii) ("judicial review shall be based on the record before the agency at the time of the determination"). In any event, as we explain, *infra*, the legislative consideration of the issue that plaintiff cited in its letter of December 6, 2006, is continuing and expedition will still serve its intended purpose.

records. As plaintiff has noted, the deadline for re-negotiating the U.S.-EU passenger data agreement is July 31, 2007. Exhibit A at 3. With respect to the ATS, congressional oversight of the program is beginning and remedial legislation was recently introduced. As Sen. Leahy explained at a recent hearing before the Senate Judiciary Committee:

> Just recently, we learned through the media that the Bush Administration has used data mining technology secretly to compile files on the travel habits of millions of law-abiding Americans. Incredibly, under the Department of Homeland Security's Automated Targeting System program ("ATS"), our government has been collecting and sharing this sensitive personal information with foreign governments and even private employers, while refusing to allow U.S. citizens to see or challenge their own so-called "terror scores." . . .
>
> I am joining with Senator Feingold, Senator Sununu and others in a bipartisan attempt to provide congressional oversight to these programs. We are introducing the Federal Agency Data Mining Reporting Act of 2007. This threshold privacy legislation would begin to restore key checks and balances by requiring federal agencies to report to Congress on their data-mining programs and activities.

Opening Statement of Senator Patrick Leahy, Senate Judiciary Committee, Hearing on "Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs," January 10, 2007 (attached hereto as Exhibit I) at 2-3.

It is thus clear that an expeditious resolution of plaintiff's entitlement to expedited processing will vindicate plaintiff's rights, notwithstanding defendant's unfavorable administrative determination. As the D.C. Circuit has observed, "stale information is of little value," *Payne Enterprises v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988), and as this Court has noted, "it seems the exceptional case where a plaintiff can litigate his case via an ordinary time-table for federal litigation and, if victorious, still attain 'expedited review' of his FOIA request." *Washington Post v. Dep't of Homeland Security*, 459 F. Supp. 2d 61, 66 (D.D.C. 2006) (footnote omitted), *appeal docketed*, No. 06-5337 (D.C. Cir. October 26, 2006). In light of the

time-sensitive nature of the right we seek to vindicate, plaintiff respectfully requests the Court's expeditious consideration and resolution of this matter.

Conclusion

For the foregoing reasons, plaintiff's motion for partial summary judgment on the issue of expedited processing should be granted.

Respectfully submitted,

/s/ David L. Sobel

DAVID L. SOBEL
D.C. Bar No. 360418

MARCIA HOFMANN
D.C. Bar No. 484136

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009
(202) 797-9009

Counsel for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

STATEMENT OF MATERIAL FACTS IN SUPPORT OF PLAINTIFF'S MOTION FOR PARTIAL SUMMARY JUDGMENT

Pursuant to Local Rule 56.1, plaintiff Electronic Frontier Foundation ("EFF" or "plaintiff") respectfully submits this statement of material facts in support of its motion for partial summary judgment.

1. In 2004, the United States ("U.S.") and the European Union ("EU") reached an agreement on the processing and transfer of Passenger Name Record ("PNR") data to DHS concerning flights between the US and EU. 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 (May 20, 2004), http://www.eurlex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf.

2. Shortly thereafter, DHS issued the "Undertakings," a set of representations reflecting how DHS (specifically, Customs and Border Protection) would collect, maintain, and secure the data. Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41543-41547.

3. The agreement was met with widespread international criticism about whether the U.S. would handle the passenger data adequately under EU privacy law. *See*, *e.g.*, Denis Staunton and Sorcha Crowley, *Civil Liberties Groups Critical of Data Deal on Flights to US*, Irish Times (Ir.), Feb. 21, 2003; Press Release, European Parliament, Parliament Defends Data Protection Rights, March 13, 2003; Andrew Orlowski, *Europe Rebuffs US Flight Info Data Grab*, The Register (UK), April 1, 2004; Sara Kehaulani Goo, *Europeans Seek Court Review of Data-Sharing Plan*, Washington Post, April 22, 2004; Nicola Smith, *MEPs Reject New Vote on EU-US Air Data Deal*, TheParliament.com (Brussels), May 4, 2004; John Lettice, *Ministers Thwart MPs, OK EU-US Airline Data Deal*, The Register (UK), May 18, 2004.

4. The European Court of Justice ruled the EU-U.S. agreement illegal under EU law in May 2006, ordering that it would become void on September 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).

5. In light of the court's decision, the U.S. and the EU worked to renegotiate the terms of the agreement.

6. In October 2006, the U.S. and the EU reached a temporary agreement on the processing and transfer of NR data to DHS from commercial airline flights between the U.S. and the EU. 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, Bureau of Customs and Border Protection (Oct. 27, 2006), http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf.

7. This understanding replaced the agreement that was reached in 2004 and subsequently found invalid by the European Court of Justice.

8. At the time the new agreement was reached, DHS sent a letter to EU officials stating that it would more broadly construe representations the agency had made in the Undertakings about how it would handle passenger data transferred between the EU and U.S. Letter to the Council Presidency and the Commission from the Department of Homeland Security of the United States of America, Concerning the Interpretation of Certain Provisions of the Undertakings Issued by DHS on 11 May 2004 in Collection with the Transfer by Air Carriers of Passenger Name Record (PNR) Data (Oct. 27, 2006), http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_letter_DHS_en.pdf.

9. Specifically, DHS intended to permit, among other things, more substantial disclosure of passenger data to other U.S. agencies with counterterrorism functions. *Id*.

10. The media reported extensively on the finalization of the temporary agreement and DHS's change in policy on how it would handle the EU-U.S. PNR data. *See*, *e.g*., Reuters, *U.S., Europe Reach Deal on Air Passenger Data*, Oct. 6, 2006; Associated Press, *Deal Reached on Passenger Data*, Oct. 6, 2006; Mark John, *U.S. to Seek More Leeway on Air Passenger Records*, Reuters, Oct. 17, 2006.

11. On November 2, 2006, defendant DHS and its component, Customs and Border Protection, published a Federal Register notice describing a "system of records" called the "Automated Targeting System" ("ATS"). 71 Fed. Reg. 64543-64546.

12. The ATS, as described by DHS, is a data-mining system that the agency uses to create "risk assessments" for tens of millions of travelers, including international travelers and U.S. citizens, based on extensive personal information. *Id*.

13. The personal data used by ATS to make determinations about travelers includes, *inter alia*, PNR data such as the records covered by the 2004 Undertakings. *Id.*

14. By letter transmitted to DHS on October 20, 2006, plaintiff requested under the FOIA agency records concerning the renegotiated agreement between the U.S. and the EU, and the handling of PNR data under the 2004 Undertakings (attached to plaintiff's memorandum of points and authorities as Exhibit A).

15. Plaintiff requested expedited processing of its FOIA request under DHS's regulations, 6 CFR § 5.5(d)(1)(ii), on the ground that the request pertained to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity," and the request was made by "a person primarily engaged in disseminating information." *Id*. at 2-3.

16. Plaintiff provided substantial evidence that it is "primarily engaged in disseminating information" and noted that it was relying upon the same evidence in support of both its "primarily engaged" claim and its asserted entitlement to classification as a "representative of the news media" for assessment of processing fees under the FOIA and 6 C.F.R. § 5.11(b)(6). *Id*. at 3.

17. In support of its assertion that there is an "urgency to inform the public" about the requested information, plaintiff noted that the agreement will have to be renegotiated before it expires in July 2007 and cited the controversy surrounding the temporary agreement, as well as the substantial news media coverage addressing it. *Id*. at 2-3.

18. By letter dated November 1, 2006, DHS denied plaintiff's request for expedited processing, asserting 1) that EFF is "not primarily engaged in the disseminating of information to the public," and 2) that EFF has not "detailed with specificity why . . . there is an urgency to

inform the public" about the Department's negotiations with the European Union with respect to the transfer of airline passenger data (attached to plaintiff's memorandum of points and authorities as Exhibit B at 1).

19. The agency also denied EFF's request to be treated as a "news media" requester for purposes of fee assessments. *Id*. at 1.

20. Plaintiff appealed the agency's adverse determinations by letter transmitted to defendant on November 21, 2006, in which it challenged both the denial of "news media" status and agency's assertion that EFF is not "primarily engaged in disseminating information" (attached to plaintiff's memorandum of points and authorities as Exhibit C at 1-2).

21. On the issue of an "urgency to inform the public" about the bi-lateral passenger data negotiations, plaintiff noted in its appeal that Homeland Security Secretary Michael Chertoff had recently underscored both the importance of, and the debate surrounding, the international exchange of passenger data (attached to plaintiff's memorandum of points and authorities as Exhibit D).

22. Plaintiff filed suit upon the agency's failure to respond to plaintiff's request for records within the 20-working-day period set forth in the FOIA, 5 U.S.C. § 552(a)(6)(A).

23. After DHS failed to timely respond to EFF's administrative appeal, plaintiff amended its complaint on December 21, 2006, to allege, *inter alia*, that defendant had unlawfully denied plaintiff's request for expedited processing.

24. By letters to DHS dated November 7, 2006, and December 6, 2006, plaintiff requested information concerning the ATS (attached to plaintiff's memorandum of points and authorities as Exhibits E & F).

25. Plaintiff requested expedited processing of both FOIA requests, stating that they meet the criteria for expedited processing under defendant DHS's regulations, 6 C.F.R. § 5.5(d)(1)(ii), because they pertain to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity," and the requests are made by "a person primarily engaged in disseminating information." Exhibit E at 2; Exhibit F at 3.

26. In both requests, plaintiff provided defendant DHS with the same evidence demonstrating that EFF is "primarily engaged in disseminating information" as plaintiff had provided in its FOIA request concerning the U.S.-EU passenger data negotiations. *Compare* Exhibits E & F *with* Exhibit A.

27. In its letter of November 7, 2006, plaintiff supported its assertion that there is an "urgency to inform the public" about the ATS by noting that there had already (just a few days after the publication of the DHS Federal Register notice) been significant news media attention devoted to the system. Plaintiff also asserted that the agency's solicitation of public comments created a compelling need for expeditious disclosure. Exhibit E at 2.

28. In its letter of December 6, 2006, plaintiff noted the extraordinary news media interest in the ATS that had occurred in a little more than a month since the publication of the Federal Register notice (which confirmed plaintiff's earlier assertion of public interest).

29. Plaintiff also noted that leading members of Congress had expressed concerns about the privacy implications of the system and announced legislative consideration of the issue. Exhibit F at 3-4.

30. By letter to plaintiff dated December 14, 2006, DHS advised plaintiff that the agency had "aggregated" plaintiff's FOIA requests dated November 7, 2006, and December 6, 2006, "to simplify processing" (attached to plaintiff's memorandum of points and authorities Exhibit G at

1).

31. Defendant further advised plaintiff that "[a]s it relates to your request for expedited treatment, your request is denied," because "you are not primarily engaged in the disseminating of information to the public," and "[you have not] detailed with specificity why you feel there is an urgency to inform the public about this topic." *Id*. at 3.

32. Plaintiff filed suit on December 19, 2006, alleging that DHS has violated the FOIA with respect to the expedited processing of plaintiff's requests submitted on November 7, 2006, and December 6, 2006.

Respectfully submitted,

/s/ David L. Sobel

DAVID L. SOBEL
D.C. Bar No. 360418

MARCIA HOFMANN
D.C. Bar No. 484136

ELECTRONIC FRONTIER FOUNDATION
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009
(202) 797-9009

Counsel for Plaintiff

Exhibit A

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

October 20, 2006

BY FACSIMILE — (571) 227-1125

Department of Homeland Security Chief FOIA Officer
Hugo Teufel
Chief FOIA Officer
The Privacy Office
Department of Homeland Security
Arlington, VA 22202

RE: Freedom of Information Act Request and
Request for Expedited Processing

Dear Mr. Teufel:

This letter constitutes an expedited request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the Department of Homeland Security ("DHS") on behalf of the Electronic Frontier Foundation ("EFF"). We make this request as part of EFF's FOIA Litigation for Accountable Government ("FLAG") Project, which works to obtain government documents and make them widely available to the public.

In 2004, the United States ("U.S.") and European Union ("EU") reached an agreement on the processing and transfer of Passenger Name Record data to DHS concerning flights between the US and EU.[1] Shortly thereafter, DHS issued the "Undertakings," a set of representations reflecting how DHS (specifically, Customs and Border Protection) would handle the data.[2] The European Court of Justice ruled the EU-U.S. agreement illegal under EU law in May 2006, ordering that it would become void on September 30.[3] In light of the decision, the U.S. and EU worked to renegotiate the terms of the agreement.

Earlier this month, the U.S. and EU reached a temporary agreement on the processing and transfer of passenger data from airlines to DHS to replace the 2004 agreement.[4] At the same time, DHS sent a letter to EU officials stating that it will interpret the 2004 Undertakings more broadly to permit, among other things, more substantial disclosure of passenger data to other U.S. agencies with counterterrorism functions.[5] Even with the new agreement in place, Reuters reported, "[t]he United States will push for more flexible arrangements with Europe on how U.S. agencies can use the personal records of air passengers to combat terrorism." Mark John, *U.S. to*

---

[1] This agreement is available at http://www.eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00840085.pdf.

[2] The Undertakings are available at http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.

[3] The court's decision is available at http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79939469C19040317&doc=T&ouvert=T&seance=ARRET.

[4] The new agreement is available at http://www.statewatch.org/news/2006/oct/eu-usa-pnr-coun-new-agreement.pdf.

[5] The letter is available at http://www.statewatch.org/news/2006/oct/eu-usa-pnr-letter-13738.pdf.

Seek More Leeway on Air Passenger Records, Reuters, Oct. 17, 2006. In the absence of further government action, the interim agreement will expire on July 31, 2007.

We are seeking the following agency records from May 30, 2006 to the present (including, but not limited to, electronic records):

1. emails, letters, reports, or other correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes;

2. emails, letters, statements, memoranda, or other correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the Undertakings;

3. records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used, disclosed to other entities, or combined with information from other sources; and

4. complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data of EU citizens.

Request for Expedited Processing

This request warrants expedited processing because it 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." 6 CFR § 5.5(d)(1)(ii).

The temporary agreement on transfer of passenger data expires on July 31, 2007, and will need to be renegotiated prior to that date. The government activity at issue here — DHS's reinterpretation of privacy commitments to the EU — raises serious questions about how DHS will implement privacy safeguards and address the privacy concerns that caused controversy even under the more protective 2004 agreement. Thus, there is a particular urgency for the public to obtain information about DHS's construction of the Undertakings under the new agreement, as well as the effectiveness of the measures in place to secure passengers' data privacy. According to the Associated Press, the "arduous" negotiations to reach the interim agreement "reflected deep divisions between the United States and the European Union over anti-terror measures and to what length governments should go in curbing personal freedoms to prevent attacks." Associated Press, *Deal Reached on Passenger Data*, Oct. 6, 2006. As Reuters noted:

> EU lawmakers raised worries that Washington was riding roughshod over data protection concerns in its quest after the 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.

Reuters, *US., Europe Reach Deal on Air Passenger Data*, Oct. 6, 2006. These issues have

attracted substantial media interest in recent days. In fact, Google News search for "privacy and 'passenger data'" returns about 621 results from news outlets throughout the world (see first page of Google News search results attached).

Indeed, the Department itself has recognized both the newsworthiness of this matter and the importance of informing the public of developments in its negotiations with the EU. On September 30, 2006, the Department issued a press release containing a statement from Secretary Chertoff concerning the negotiations.[6]

The purpose of this request is to obtain information directly relevant to DHS's guidelines on the handling of EU-US passenger data before July 31, 2007, when the temporary agreement is set to expire. The records requested involve the manner in which DHS is construing its policies on this matter, and clearly meet the standard for expedited processing. There is clearly "an urgency to inform the public" about the Department's policies with respect to this issue in order to facilitate a full and informed public debate on the U.S. position in the upcoming bi-lateral negotiations.

Further, as I explain below in support of our request for "news media" treatment, EFF is "primarily engaged in disseminating information."

Request for News Media Fee Status

EFF asks that it not be charged search or review fees for this request because EFF qualifies as a representative of the news media pursuant to the FOIA and 6 C.F.R. § 5.11(b)(6).

EFF is a non-profit public interest organization that works "to protect and enhance our core civil liberties in the digital age."[7] One of EFF's primary objectives is "to educate the press, policymakers and the general public about online civil liberties."[8] To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

First, EFF maintains a frequently visited web site, http://www.eff.org, which received 40,681,430 hits in September 2006 — an average of 56,501 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.

EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 77,000 subscribers. A complete archive of past EFFectors is available at http://www.eff.org/effector/.

Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (http://www.eff.org/deeplinks/) reports and analyzes newsworthy developments in

---

[6] This press release is available at http://www.dhs.gov/xnews/releases/pr_1159893986311.shtm.

[7] Guidestar Basic Report, Electronic Frontier Foundation, http://www.guidestar.org/pqShowGsReport.do?npoId=561625 (last visited Oct. 16, 2006).

[8] *Id.*

technology. It also provides miniLinks, which direct readers to other news articles and commentary on these issues. DeepLinks had 538,297 hits in September 2006.[9]

In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than eighteen white papers published since 2002. These papers, available at http://www.eff.org/wp/, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.

EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (http://www.powells.com). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (http://www.amazon.com). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at http://cryptome.org/cracking-des.htm and for sale at Amazon.com.

Most recently, EFF has begun broadcasting podcasts of interviews with EFF staff and outside experts. *Line Noise* is a five-minute audio broadcast on EFF's current work, pending legislation, and technology-related issues. A listing of *Line Noise* podcasts is available at feed://www.eff.org/rss/linenoisemp3.xml and feed://www.eff.org/rss/linenoiseogg.xml. These podcasts were downloaded more than 1,300 times from EFF's web site last month.

Request for a Public Interest Fee Waiver

EFF is entitled to a waiver of duplication fees because disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(a)(iii) and 6 C.F.R. § 5.11(k). To determine whether a request meets this standard, Department of Homeland Security components determine whether "[d]isclosure of the requested information is likely to contribute significantly to public understanding of the operations or activities of the government," and whether such disclosure "is not primarily in the commercial interest of the requester." 6 C.F.R. §§ 5.11(k)(i), (ii). This request clearly satisfies these criteria.

First, DHS's handling of passenger data from EU-U.S. flights concerns "the operations or activities of the government." 6 C.F.R. § 5.11(k)(2)(i). DHS is a government agency, and its use of passenger data to make determinations about travelers unquestionably constitutes government operations or activities.

Second, disclosure of the requested information will "contribute to an understanding of government operations or activities." 6 C.F.R. § 5.11(k)(2)(ii) (internal quotation marks omitted). EFF has requested information that will shed light on the manner in which DHS uses passenger data to screen travelers entering the United States, as well as the subsequent retention,

[9] These figures include hits from RSS feeds through which subscribers can easily track updates to DeepLinks and miniLinks.

uses, and disclosures of that data.

Third, the requested material will "contribute to public understanding" of DHS's handling of EU-U.S. passenger data. 6 C.F.R. § 5.11(k)(2)(iii) (internal quotation marks omitted). This information will contribute not only to EFF's understanding of DHS's passenger data policies, but to the understanding of a reasonably broad audience of persons interested in the subject. EFF will make the information it obtains under the FOIA available to the public and the media through its web site and newsletter, which highlight developments concerning privacy and civil liberties issues, and/or other channels discussed more fully above.

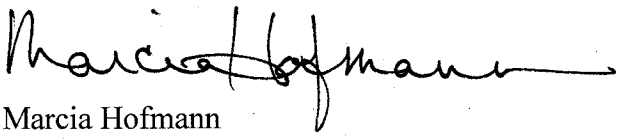
Fourth, the disclosure will "contribute significantly" to the public's knowledge and understanding of how DHS handles EU-U.S. passenger data. 6 C.F.R. § 5.11(k)(2)(iv) (internal quotation marks omitted). Disclosure of the requested information will help inform the public about the contours of the new agreement and DHS's interpretation of the Undertakings, as well as contribute to the public debate about the adequacy of these policies under EU law.

Furthermore, a fee waiver is appropriate here because EFF has no commercial interest in the disclosure of the requested records. 6 C.F.R. § 5.11(k)(3). EFF is a 501(c)(3) nonprofit organization, and will derive no commercial benefit from the information at issue here.

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact me at (202) 797-9009 x. 12. As the FOIA provides, I will anticipate a determination on our request for expedited processing within ten (10) calendar days.

Under penalty of perjury, I hereby affirm that the foregoing is true and correct to the best of my knowledge.

Sincerely,



Marcia Hofmann
Staff Attorney

Results **1** - **10** of about **621** for **privacy and passenger-data**. (**0.06** 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

EU-US deal on airline **passenger data** deal could set world standard **...**

International Herald Tribune, France - 5 hours ago

... The agreement, reached after months of wrangling over **privacy** rights, gives American law enforcement agencies continued access to **passenger data** on US-bound **...**

US to seek more leeway on air passenger records Washington Post
Deal sealed over air **passenger data** release The Australian
EU formally signs new trans-Atlantic air **passenger data** deal with **...** International Herald Tribune
Raw Story
all 36 news articles »

EU signs interim air **passenger data**-sharing deal with US

JURIST - 16 hours ago

... information [Reuters report; DHS press release] without violating EU **privacy** laws **...** of Homeland Security [official website] to ask for **passenger data**, rather than **...**

US wants more freedom on use of EU air **passenger data**

EUobserver.com, Belgium - 32 minutes ago

... airlines to provide US authorities with 34 types of **passenger data**, including names **...** In return, the US has committed to respect **privacy** protection safeguards **...**

EU: the air **passenger data** transfer agreement has been

Avionews, Italy - 5 hours ago

... airlines will keep on communicating passengers' personal data to the American security authorities, which undertook to warrant European citizens' **privacy**. **...**

EU Parliament To Fight **Passenger Data Privacy** Agreement

CSO, MA - Oct 12, 2006

... parliamentarians are gearing up for a fight over data **privacy**, after justice **...** signed a new temporary agreement to pass over airline **passenger data** to American **...**

US, Europe to Share Air **Passenger Data**

AMTOnline.com, MD - Oct 9, 2006

... Friday on sharing trans-Atlantic air **passenger data** for anti-terrorism investigations, concluding arduous talks that highlighted divisions over **privacy** rights. **...**

Exhibit B

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

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

Homeland Security

Privacy Office DHS-D3

November 1, 2006

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, N.W.
Suite 650
Washington, DC 20009

Re: **DHS/OS/PRIV 07-90/Hofmann request**

Dear Ms. Hofmann:

This acknowledges receipt of your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated October 20, 2006, seeking the following DHS records from May 30, 2006 to the present:

1. All correspondence from DHS officials to European Union officials concerning the transfer and use of passenger data from air carriers to the US for prescreening purposes.
2. All correspondence from DHS officials to U.S. government officials or employees interpreting or providing guidance on how to interpret the undertakings.
3. Records describing how passenger data transferred to the U.S. under the temporary agreement is to be retained, secured, used disclosed to other entities, or combined with information from other sources.
4. Complaints received from EU citizens or official entities concerning DHS acquisition, maintenance and use of passenger data from EU citizens.

We are holding your fee waiver request in abeyance pending the quantification of responsive records. In the event that your fee waiver request is denied, we shall charge you for records in accordance with the DHS Interim FOIA regulations as they apply to non-commercial requestors. As a non-commercial requestor you will be charged 10-cents a page for duplication, although the first 100 pages are free, as are the first two hours of search time, after which you will pay the per quarter-hour rate of the searcher. We will construe the submission of your request as an agreement to pay up to $25.00. You will be contacted before any further fees are accrued.

As it relates to your request for expedited treatment, your request is denied. Pursuant to 5 U.S.C. §§552 (a)(6)(E)(i), each agency shall promulgate regulations providing for expedited processing of records. Accordingly, §5.5(d) of the DHS Interim FOIA and Privacy Act regulations, 6 C.F.R. Part 5, addresses the Department's criteria for granting expedited treatment. You do not qualify for either category. Clearly, the lack of expedited treatment in this case will not pose an imminent threat to the life or physical safety of an individual. In addition, you are not primarily engaged in the disseminating of information to the public, nor have you detailed with specificity why you feel there is an urgency to inform the public about this topic. This urgency would need to exceed the public's right to know about government activity

generally. Finally, you 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.

If you deem the decision to deny expedited treatment of your request an adverse determination, you may exercise your appeal rights. Should you wish to do so, you must send your appeal within 60 days of receipt of this letter to the following address: Office of General Counsel, Department of Homeland Security, Washington, D.C. 20528, following the procedures outlined in Subpart A, Section 5.9, of the DHS Regulations. Your envelope and letter should be marked "Freedom of Information Act Appeal." Copies of the DHS regulations are available at: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0318.xml.

In addition, we are referring your request to the Acting FOIA Officer for U.S. Customs and Border Protection (CBP), Richard Chovanec, (Mint Annex-5th Floor) 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229, who will forward your request on for processing to the appropriate office within CBP. Please note that our decision regarding your request for a fee waiver and expedited processing applies to this office only, and CBP will issue a separate determination upon receipt of your request.

As it relates to this office, your request has been assigned reference number **DHS/OS/PRIV 07-90/Hofmann request**. Please refer to this identifier in any future correspondence. We have queried the appropriate component of DHS for responsive records. If any responsive records are located, they will be reviewed for determination of releasability.

Per §5.5(a) of the DHS FOIA regulations, 6 C.F.R. Part 5, the Department processes FOIA requests according to their order of receipt. We will make every effort to comply with your request in a timely manner; however, there are currently 61 open requests ahead of yours. Nevertheless, please be assured that one of the processors in our office will respond to your request as expeditiously as possible.

Sincerely,

Catherine M. Papoi
Acting Director, Departmental Disclosure & FOIA

Exhibit C

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 21, 2006

BY FACSIMILE – 571-227-4171

Associate General Counsel
Office of General Counsel
Department of Homeland Security
Washington, DC 20528

RE: Freedom of Information Act Appeal; DHS/OS/PRIV 07-90

To Whom It May Concern:

This letter constitutes an appeal pursuant to 5 U.S.C. § 552(a)(6)(E)(ii)(II). The Electronic Frontier Foundation ("EFF") appeals an initial determination issued on November 1, 2006, by Catherine M. Papoi, Acting Director, Departmental Disclosure & FOIA, with respect to the above-numbered request (attached hereto). Specifically, Ms. Papoi denied EFF's request to be treated as a "news media" requester for purposes of fee assessments, and denied its request for expedited processing of its FOIA request.

Entitlement to "News Media" Fee Assessment

In her letter, Ms. Papoi stated that unless EFF is granted a fee waiver, "we shall charge you for records in accordance with the DHS Interim FOIA regulations as they apply to non-commercial requestors," *i.e.*, fees will be assessed for both search and duplication. Ms. Papoi further states that the agency "will construe the submission of your request as an agreement to pay up to $25.00." By this letter, EFF is notifying the agency that it does *not* agree to pay *any* fees related to search time.

In our request letter of October 20, 2006, we provided extensive information in support of EFF's entitlement to "news media" status for purposes of fee assessments. That letter is incorporated herein by reference. In order to update the information we previously submitted, I am attaching hereto a copy of EFF's most recent newsletter, which includes coverage and analysis of issues such as electronic voting problems in the recent mid-term election, new developments in intellectual property law, a Federal Register notice published by DHS, and legislative and judicial consideration of the National Security Agency's surveillance program. I also note that since the newsletter was published last week, EFF's news blog (www.eff.org/deeplinks/) has covered additional news items, including a decision issued yesterday by the California Supreme Court concerning liability for information posted on the Internet. It is clear that this material, which EFF publishes on a regular and continuous basis, constitutes "news" within the meaning of the agency's regulations. 6 C.F.R. § 5.11(b)(6) ("The term 'news' means information that is about current events or that would be of current interest to the public."). EFF's publication of this material, *inter alia*, clearly qualifies it for classification as a "news

1875 Connecticut Ave., NW · Suite 650 · Washington, DC 20009
202 797 9009 202 797 9066 www.eff.org information@eff.org

media" entity within the meaning of the regulations. *Id.* ("Examples of news media entities include . . . publishers of periodicals . . . who make their products available for purchase or subscription by the general public.").

Entitlement to Expedited Processing

Ms. Papoi denied EFF's request to expedite the processing of its FOIA request on two grounds: 1) that EFF is "not primarily engaged in the disseminating of information to the public," and 2) that EFF has not "detailed with specificity why . . . there is an urgency to inform the public" about the Department's negotiations with the European Union with respect to the transfer of airline passenger data. With respect to the dissemination issue, I incorporate by reference the information we have provided with respect to EFF's entitlement to "news media" status.

As for the "urgency" issue, Ms. Papoi asserted that EFF has not "offer[ed] any evidence of public interest that is greater than the public's general interest in the transfer and use of passenger name data." In appealing from that determination, I reiterate and incorporate the information initially provided to the agency in support of EFF's FOIA request. In addition, and to update the relevant "evidence," I note that Secretary Chertoff delivered a speech to the Federalist Society on November 17, in which he saw fit to highlight the dispute between the United States and the EU on passenger data. *See* http://www.dhs.gov/xnews/speeches/sp_1163798467437.shtm. The full text of that speech is incorporated herein by reference, and I specifically note the Secretary's acknowledgement that the privacy issues surrounding the transfer of passenger data "led to a very substantial debate." *See also* Reuters, "Chertoff says U.S. threatened by international law," November 17, 2006 (attached hereto). It is precisely the "substantial debate" the Secretary noted that establishes the public interest in the requested material. EFF is clearly entitled to the expedited processing of its request.

As the FOIA and DHS regulations require, I look forward to your expeditious resolution of this appeal. Feel free to contact me at (202) 797-9007 ext. 10 if I can provide you with additional information.

Sincerely,

David L. Sobel
Senior Counsel

attachments

EFFector Vol. 19, No. 42 November 15, 2006 editor@eff.org

A Publication of the Electronic Frontier Foundation
ISSN 1062-9424

In the 403rd Issue of EFFector:

For more information on EFF activities & alerts:
<http://www.eff.org/>

Make a donation and become an EFF member today!
<http://eff.org/support/>

Tell a friend about EFF:
http://action.eff.org/site/Ecard?ecard_id=1061

effector: n, Computer Sci. A device for producing a desired change.

:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:

* Don't Let Lame Duck Congress Pass NSA Spying Bills!

On Election Day, Americans fired many members of Congress who wanted to rubberstamp the NSA's illegal surveillance program. But before newly-elected representatives can take office and defend your rights, the president wants to sneak through spying legislation -- including a proposal that could threaten cases like EFF's lawsuit against AT&T. Your representatives are among the key decision makers on this issue, and it's critical that you take action now to block these bills:
<http://action.eff.org/fisa>

Lawsuits against the telephone providers may provide the best chance to stop the spying program, and no one should be let off the hook for such blatant violation of the law. Yet members of Congress are now pushing legislation that purports to immunize telephone companies and other corporations that illegally collaborated with the government's spying program.

Instead of letting the next Congress and the American public have a real debate about this issue, lame duck representatives may try to attach these proposals to a variety of bills. Don't let them get away with it -- visit our Action Center, and voice your opposition now:

<http://action.eff.org/fisa>

For more on EFF's case against AT&T:
<http://www.eff.org/legal/cases/att/>

: . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . :

* Judge to Consider Next Steps in AT&T Case

EFF to Fight Against Spying Case Delays in Friday Hearing

San Francisco - On Friday, September 17, at 10:30 a.m., a federal judge in San Francisco will consider the next steps in EFF's class-action lawsuit against AT&T.

EFF's suit accuses the telecom giant of collaborating with the National Security Agency (NSA) in illegal spying on millions of ordinary Americans. Other cases recently transferred to U.S. District Court Judge Vaughn Walker's courtroom include similar allegations.

The U.S. government has intervened in EFF's case, contending that even if the NSA program is illegal, the lawsuit should be dismissed because it might expose state secrets. Last week, the U.S. government asked the judge to halt all proceedings until the 9th U.S. Circuit Court of Appeals rules on motions to dismiss the case.

Friday's case management conference will address how EFF's suit and the other class-action cases might go forward without implicating the state secrets privilege and what discovery should proceed during the appeals process.

For more information about attending the hearing, please contact press@eff.org.

WHAT:
Hepting v. AT&T and other NSA telecommunications records lawsuits

WHEN:
Friday, November 17, 10:30 a.m.

WHERE:
450 Golden Gate Ave., Courtroom 6
San Francisco, CA 94102

For more on EFF's case against AT&T:
<http://www.eff.org/legal/cases/att/>

For this release:
<http://www.eff.org/news/archives/2006_11.php#005003>

: . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . :

* Lowering DRM Flags in Lame Duck?

Variety's Multichannel News reports that the telecommunications reform bill hangs in limbo after last week's election and is unlikely to be at the forefront in the next Congress. The Senate's version had been home to the broadcast and audio flag digital rights management (DRM)

mandates, so Hollywood and the recording industry may have to seek new ways to sneak through restrictions on your digital television and radio devices next year.

But this year's fight isn't over yet -- there might be one last push for these proposals in the lame duck session, as Public Knowledge's Gigi Sohn points out in a recent blog post. If the entertainment industry tries attaching the proposals to appropriations bills, it won't be the first time.

Regardless, we can expect these dangerous DRM mandates to rear their ugly heads in some form next year.

For this post and more related links:
<http://www.eff.org/deeplinks/archives/004998.php>

: :

* E-Voting Problems in Tight Florida Race

According to vote tallies, more than one in eight voters did not select a candidate in Sarasota County, Florida's Congressional race. Seems fishy, no? Sadly, problems with electronic voting machines may be responsible for the undervote, and, in a race separated by a mere 373 votes, design flaws might be the difference maker. Voters in that county chose last week to scrap the machines in favor of paper ballots by 2008, but that can't remove the shadow e-voting machines cast over this election.

For our initial report on this race:
<http://www.eff.org/deeplinks/archives/004993.php>

For the Orlando Sentinel's recent update on the race:
<http://www.orlandosentinel.com/news/local/state/orl-voterprobs1206nov12,0,6657404.story?coll=orl-news-headlines-state>

Of course, Sarasota isn't the only close race impacted by e-voting machines. Down over 7,000 votes to Democratic challenger Jim Webb, Virginia Senator George Allen conceded the race without a recount, but the fact remains that a full and thorough recount wasn't even possible. The majority of Virginia counties use touchscreen voting machines, and most of those counties use machines that do not generate voter-verified paper ballots. Instead of creating anything truly useful for officials to recount, the machines simply reproduce data that is already in memory, in effect reprinting the results rather than recounting ballots in any meaningful sense.

Read more about e-voting in Virginia:
<http://www.eff.org/deeplinks/archives/004996.php>

Those are just some of the many e-voting problems in Election 2006. Hopefully, they demonstrate once and for all that reform is needed to make sure every vote counts -- take action now to protect your right to vote:
<http://action.eff.org/site/Advocacy?id=109>

For more on e-voting in this election:
<http://www.eff.org/news/archives/2006_11.php#004991>

:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:

* Brief Urges Supreme Court to Tackle Secret Law

Americans Have the Right to See Laws They Must Follow

San Francisco - EFF and a coalition of non-profit organizations asked the U.S. Supreme Court Monday to hear a case challenging a secret law governing travelers in American airports.

The case centers on the Transportation Security Agency (TSA) requirement that travelers show identification before boarding commercial aircraft. So far, the TSA has refused to disclose the terms of the identification requirement to the public, claiming that they are "sensitive security information." In the amicus brief urging the Supreme Court to hear Gilmore v. Gonzales, EFF demonstrates that Congress never intended agencies to have unfettered discretion to impose requirements upon the public without allowing the public to review them.

"The TSA is allowed to withhold some information from the public, but only in cases where transportation security is at risk," said EFF Staff Attorney Marcia Hofmann. "Simply showing Americans the rules they must follow can't possibly compromise security. The real danger here is meaningless secrecy, which can hide security flaws, frustrate the justice system, create confusion, and undermine government accountability."

The Constitution and laws like the Freedom of Information Act (FOIA) prohibit the government from imposing secret laws on the public. But if the lower court decision permitting the secrecy is allowed to stand, it opens the door to other government agencies creating undisclosed rules and regulations without oversight.

"'Security' shouldn't be a magic password allowing the government to escape accountability," said Hofmann. "The Supreme Court should hear this case and review why the TSA insists on keeping this basic information secret."

The amicus brief was also signed by the American Association of Law Libraries, American Library Association, Association of Research Libraries, Center for Democracy and Technology, National Security Archive, Project on Government Secrecy of the Federation of American Scientists, and Special Libraries Association.

For the full amicus brief:
<http://www.eff.org/legal/cases/gilmore_v_gonzales/gilmore_amicus.pdf>

For this release:
<http://www.eff.org/news/archives/2006_11.php#005000>

:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:

* Landmark Education DMCA Case Update

EFF recently announced that it was fighting against Landmark

Education's campaign to identify individuals who posted a French documentary, entitled Voyage Au Pays Des Nouveaux Gourous (Voyage to the Land of the New Gurus), that was critical of the Landmark program and included hidden camera footage from inside a Landmark Forum event in France.

EFF is currently talking with Landmark in an attempt to reach an amicable resolution about Landmark's Digital Millennium Copyright Act (DMCA) subpoena to Google. In the hope that we can resolve this without need of litigation, EFF has held off on filing its motion to quash that subpoena.

In the mean time, Landmark responded to our press release, according to Red Herring magazine:

"While we appreciate the work of the EFF, the allegation that our copyright claim is bogus is entirely inaccurate," [Art Schreiber, general counsel for Landmark Education] said. "The facts are clear that the Landmark Forum program has for many years been copyrighted. Materials covered by this copyright registration were included throughout the video."

While we appreciate the kind words, we disagree with Mr. Schreiber's copyright analysis. To the extent that the documentary includes any materials copyrighted by Landmark, that use is clearly for purposes of criticism and commentary, i.e., a non-infringing fair use. Yesterday we released a draft of our motion to quash, which explains in detail why Landmark's copyright claim does not hold water. Indeed, it's not even a close call. Sorry, Landmark, but your claim is still bogus.

For this post and related links:
<http://www.eff.org/deeplinks/archives/004994.php>

:.:.:.:.:.:.:.:.:.:.:.:.:.:.:

* Help Bust Two Bad Patents!

EFF's Patent Busting Project fights back against bad patents by filing requests for reexamination against the worst offenders. We've successfully pushed the Patent and Trademark Office to reexamine patents held by Clear Channel and Test.com, and now we need your help to bust a few more.

A company called NeoMedia has a patent on reading an "index" (e.g, a bar code) off a product, matching it with information in a database, and then connecting to a remote computer (e.g., a website). In other words, NeoMedia claims to have invented the basic concept of any technology that could, say, scan a product on a supermarket shelf and then connect you to a price-comparison website. To bust this overly broad patent, we need to find prior art that describes a product made before 1995 that might be something like a UPC scanner, but which also connects the user to a remote computer or database. Take a look at the description and please forward it to anyone you know who might have special knowledge in this area:
<http://www.eff.org/patent/wanted/prior.php?p=neomedia>

You can send your prior art tips in here:
<http://www.eff.org/patent/wanted/contribute.php?p=neomedia>

Also in our sights is a patent on personalized subdomains from Ideaflood. For example, a student named Alice might have personalized URL "http://alice.university.edu/" that redirects to a personal directory at "http://www.university.edu/~alice/." Ideaflood says that it has a patent on a key mechanism that makes this possible. We need prior art that describes such a method being used before 1999, specifically using DNS wildcards, html frames, and virtual hosting. Prior art systems might have existed in foreign ISPs, universities, or other ISPs with web-hosting services. You can find the prior art description here:
<http://www.eff.org/patent/wanted/prior.php?p=ideaflood>

And please send tips in here:
<http://www.eff.org/patent/wanted/contribute.php?p=ideaflood>

For more on the Patent Busting Project:
<http://www.eff.org/patent/>

: . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . :

* Homeland Security to "Target" Millions in Data-Mining System

The Department of Homeland Security (DHS) recently published a notice in the Federal Register disclosing the existence of a "new system of records" -- the Automated Targeting System (ATS) -- that assigns "risk assessments" to millions of U.S. citizens who seek "to enter or exit the United States" or whose work involves international trade. The system appears to involve the data-mining of massive amounts of information derived from a wide variety of sources, including Passenger Name Record (PNR) data obtained from commercial air carriers.

The "risk assessments" generated by the system will be retained for "up to forty years," according to DHS, in order to "cover the potential lifespan of individuals associated with terrorism or other criminal activity." But wait -- just because you're currently innocent, that doesn't mean you get a free pass. As the notice goes on to explain:

"All risk assessments need to be maintained because the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified."

DHS has exempted all of the data contained in the ATS from the "access" and "correction" requirements of the Privacy Act of 1974, which means that citizens have no right to learn about their own "risk assessments" or to challenge them. Franz Kafka, call your office.

For this post and related links:
<http://www.eff.org/deeplinks/archives/004980.php>

: . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . :

* Sun Releases Java Under GPL

This week, Sun Microsystems announced that it is releasing the Java source code under the GPL free software license, meaning anyone is free to copy, redistribute, modify, and make many other uses of the code. Free Software Foundation founder Richard Stallman hailed the release as one of the most significant software contributions by any company to the free software community. ZDNet and Sun's site have more details:
<http://blogs.zdnet.com/Burnette/?p=199>
<http://www.sun.com/2006-1113/feature/index.jsp>

: . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . : . :

* Nominate a Pioneer for EFF's 2007 Pioneer Awards!

EFF established the Pioneer Awards to recognize leaders on the electronic frontier who are extending freedom and innovation in the realm of information technology. This is your opportunity to nominate a deserving individual or group to receive a Pioneer Award for 2007.

The International Pioneer Awards nominations are open both to individuals and organizations from any country. Nominations are reviewed by a panel of judges chosen for their knowledge of the technical, legal, and social issues associated with information technology.

How to Nominate Someone for a 2007 Pioneer Award:

You may send as many nominations as you wish, but please use one email per nomination. Please submit your entries via email to pioneer@eff.org. We will accept nominations until January 15, 2007.

Simply tell us:

1. The name of the nominee,

2. The phone number or email address or website by which the nominee can be reached, and, most importantly,

3. Why you feel the nominee deserves the award.

Nominee Criteria:

There are no specific categories for the EFF Pioneer Awards, but the following guidelines apply:

1. The nominees must have contributed substantially to the health, growth, accessibility, or freedom of computer-based communications.

2. To be valid, all nominations must contain your reason, however brief, for nominating the individual or organization and a means of contacting the nominee. In addition, while anonymous nominations will be accepted, ideally we'd like to contact the nominating parties in case we need further information.

3. The contribution may be technical, social, economic, or cultural.

4. Nominations may be of individuals, systems, or organizations in the private or public sectors.

5. Nominations are open to all (other than current members of EFF's staff and board or this year's award judges), and you may nominate more than one recipient. You may also nominate yourself or your organization.

6. Persons or representatives of organizations receiving an EFF Pioneer Award will be invited to attend the ceremony at EFF's expense.

More on the EFF Pioneer Awards:
<http://www.eff.org/awards/pioneer/>

: :

* miniLinks
The week's noteworthy news, compressed.

~ Universal CEO: Pirates Are to Pirate Ships, as Fans Are to iPods
"These devices are just repositories for stolen music, and they all know it," Doug Morris says.
<http://www.billboard.com/bbcom/news/article_display.jsp?vnu_content_id=1003380831>

~ RIAA Explodes at Claim That It's Unfriendly to Fair Use
Cary Sherman claims consumer electronics industry is "extremist."
<http://techdirt.com/articles/20061113/082502.shtml>

~ Europe-based Legal Advice for Free Software Developers
New "Freedom Task Force" will be based in Zurich, Switzerland, advising and enforcing the GPL.
<http://mail.fsfeurope.org/pipermail/press-release/2006q4/000159.html>

~ Crimson Tide of Litigation
University of Alabama asks court to forbid artist from using "famous crimson and white color scheme."
<http://www.nytimes.com/2006/11/12/us/12artist.html>

~ GNU's Not Anti-trust
Full judicial opinion and commentary on Daniel Wallace's attempt to have the GPL declared anti-competitive.
<http://williampatry.blogspot.com/2006/11/gnu-gnu.html>

~ Does Opt-Out Copyright Violate First Amendment?
Larry Lessig's Kahle v. Gonzales is heard by the Ninth Circuit.
<http://www.lessig.org/blog/archives/003602.shtml>

~ ITU Makes Bid to Control "Security in Cyberspace"
The new secretary general of the UN's ITU Telecoms Development Bureau, Hamadoun Toure, wants to take the lead in governing security issues online.
<http://publicaffairs.linx.net/news/?p=598>

~ Who's Censoring Whom?
State Net censorship monitors the OpenNet Initiative talks to Wired News.
<http://www.wired.com/news/technology/0,72104-0.html>

: :

* Administrivia

EFFector is published by:

The Electronic Frontier Foundation
454 Shotwell Street
San Francisco CA 94110-1914 USA
+1 415 436 9333 (voice)
+1 415 436 9993 (fax)
<http://www.eff.org/>

Editor:
Derek Slater, Activist
derek@eff.org

Membership & donation queries:
membership@eff.org

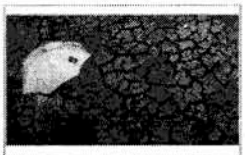
General EFF, legal, policy, or online resources queries:
information@eff.org

Current and back issues of EFFector are available via the Web at:
<http://www.eff.org/effector/>

Click here to unsubscribe or change your subscription preferences:
http://action.eff.org/site/CO?i=VAl6AE99lkZCizU2FCaj3zG7bj4AmTE3&cid=1041

Click here to change your email address:
http://action.eff.org/addresschange

This newsletter is printed on 100% recycled electrons.



Chertoff says U.S. threatened by international law

17 Nov 2006 23:15:21 GMT
Source: Reuters

By David Morgan

WASHINGTON, Nov 17 (Reuters) - A top Bush administration official on Friday said the European Union, the United Nations and other international entities increasingly are using international law to challenge U.S. powers to reject treaties and protect itself from attack.

"International law is being used as a rhetorical weapon against us," Homeland Security Secretary Michael Chertoff, a former federal appellate judge, said in a speech to the Federalist Society, a conservative policy group.

Chertoff cited members of the European Parliament in particular as harboring an "increasingly activist, left-wing and even elitist philosophy of law" at odds with American practices and interests.

But he said the same pattern could be seen in the policies of the United Nations and other international bodies.

"What we see here is a vision of international law that if taken aggressively would literally strike at the heart of some of our basic fundamental principals -- separation of powers, respect for the Senate's ability to ratify treaties and ... reject treaties," Chertoff said.

President George W. Bush's administration has been repeatedly criticized by rights groups and foreign governments, including some allies, over some of the tactics it has used in Washington's war on terrorism since the Sept. 11 attacks.

Critics have aimed at Bush's policies such as the indefinite detention of foreign terrorism suspects at the Guantanamo Bay prison in Cuba.

Chertoff said the U.S. Supreme Court decision on Guantanamo prisoner Salim Ahmed Hamdan that required the United States to treat detainees under Geneva Conventions standards showed international law's entry into the U.S. domain.

He also pointed to negotiations leading up to last month's interim agreement between the United States and the European Union on sharing personal information about trans-Atlantic airline passengers.

The Bush administration sought addresses, credit card details, phone numbers and other details for U.S.-bound European air passengers as a way to determine whether any should be turned back from entering the United States as a security risk.

"Some in the European Parliament argued that the fact the information was derived from Europeans coming to the U.S. meant that we should be forced in the United States to let Europe supervise and set the terms of how we make use of that information," Chertoff said.

"Fortunately, we resolved it in a way that does address the principal concerns that we have," he added.

Chertoff also cited press reports of European privacy activists trying to constrain U.S. use of financial information obtained in Washington's war on terrorism.

"There are increasing efforts to control our use of information in our own country," he said.

Some EU activists, he said, believe national sovereignty is weakening under an avalanche of international laws.

"It (is) a chilling vision of where we could go, given the current developments in international and transnational law," Chertoff said.

Exhibit D

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Homeland Security

Remarks by the Secretary of Homeland Security Michael Chertoff at the Federalist Society's Annual Lawyers Convention

Release Date: November 17, 2006

Washington, D.C.
Federalist Society's Annual Lawyers Convention

Secretary Chertoff: Thank you very much. A lot of lawyers in this room. Now I don't usually address lawyers' groups anymore because one of the benefits of my current position is it's the first job I've had since I graduated from law school in which I wasn't acting in a capacity of being a lawyer. And I'll tell you, it's wonderful. Every time there's a problem, I say, go ask the lawyers about that.

But I am delighted to speak to this group because I think the premise of the Federalist Society is that ideas matter in the world of the law and that our views of the role of the courts and our philosophy of law actually has a real-world impact on the way we organize our lives and conduct our daily affairs.

Now when I was in school, in law school -- and I graduated in 1978 -- I don't think the Society had yet been formed. And when I was in school, during the period from '75 to '78, we were still in the, I would say, full flush of the Warren Court years when the phrase "judicial activism" was viewed as a term of admiration. And for those of you who are younger, it may be a little hard to imagine what it was like to be in an environment in which there were only very few of us who were willing to talk about things like judicial restraint, or suggest that judges couldn't solve every single problem, and to be facing really a majority that looked at us like we were demented.

One of those who was a year behind me, but I think probably had as a very similar experience, was John Roberts, now the Chief Justice. There were very few people, frankly, who in my era were in a position to argue seriously for what Chief Justice Roberts has, I think very accurately, described as "judicial modesty."

First, let me tell you what I mean, or what I think the phrase "judicial modesty" means. I think it means things like deferring to the political branches that represent the will of the people. I think it means cautiousness in the use of judicial remedies and kind of a humble recognition in the fact that sometimes there can be unintended consequences. I think it means mindfulness of the limits of judicial competence.

You know, judges are -- by and large -- pretty smart. When I was a judge, my colleagues were pretty smart, but they're not necessarily great at everything, and they don't necessarily understand everything. And they kind of -- a modesty in understanding their own competence is, to me, a significant element of the right way a judge out to behave.

And, of course, a critical element in judicial modesty is a rigorous observance of the self-limiting elements of jurisdiction. You have to be particularly careful about policing yourself to make sure you don't overstep because judges, after all, are generally given the last word about jurisdiction.

So what I think is really fascinating about the society is that by forming the Federalist Society, the visionaries who created the organization established fora in which these ideas of judicial modesty could be openly discussed in a collegial environment. Essentially, they created a counterweight to the prevailing academic orthodoxy of the '60s and '70s, and that was a very positive thing.

Of course, some people now have taken up the idea that really the Federalist Society is kind of like a modern day Da Vinci conspiracy -- a secret society that controls all the legal jobs and all the legal decision-making in the administration -- and of course, we know that is nonsense. But what the society did was it did create a forum in which one could challenge ideas that had previously been accepted as the conventional wisdom.

I'm not going to say that that means that the philosophy of judicial modesty or similar conservative philosophies now dominate the legal landscape. Far from it, many people still believe -- whether they be in academia, or on the courts, or practicing law -- many still believe that the purpose of the courts is to pursue a vision of the good life of social

justice as conceived by legal thinkers and judges.

But now, in large part because of the work that the society and others have done, the claim for judicial modesty is sufficiently well established that everybody understands, even the critics of that claim, that they have to take it seriously and they have to address it. Judges and lawyers who take an activist approach realize that they have to respond to the critique of that activism. Conservatism and judicial modesty have now become forces to be reckoned with in the intellectual discourse of the law here in the United States. In short, you've leveled the playing field, and that has been a very good thing.

So now your work is not done because I'm going to ask you to confront a new challenge, and that is the rise of an increasingly activist, left-wing, and even elitist philosophy of law that is flourishing not in the United States but in foreign courts and in various international courts and bodies.

For decades, the judges, the lawyers and the academics who provide the intellectual firepower in the development of international law and transnational law have increasingly advocated for a broad vision of legal activism that exceeds even the kind of legal activism we saw discussed in the academy here in the United States in the 60s.

So now you're scratching your head and you're asking yourself, why does the Secretary of Homeland Security care about this? Well, in my domain, much of what I do actually intertwines with what happens overseas. And what happens in the world of international law and transnational law increasingly has an impact on my ability to do my job and the ability of the people who work in my department to do their jobs. And I'll give you a recent example.

Some of you may have followed in the press that there was a difference of opinion between the European Union and the United States about the use of something called passenger name record data, which is basic information that you get when you buy a ticket or you work through a travel agent as part of the process of planning your trip to come to the United States. There is great value to us in the ability to get access to that information as part of the process of our determining who we are going to allow to enter the United States. That, of course, is a fundamental core power of any sovereign; you get to decide who you're going to admit and who you're going to reject.

And it turns out that this very modest amount of information, like your address, and your credit card, and your telephone number, are very useful for us in identifying whether people seeking to come into the country have connections to terrorists that, at a minimum, suggest we ought to put them into secondary before we grant them admission. And this strikes me as eminently reasonable, and I can tell you it is a critical tool in protecting this country.

But privacy advocates, particularly in the European Parliament believe that because that information is collected in, among other places, Europe, they should determine how we use that information in deciding who is going to be allowed into our country. And this led to a very substantial debate. Fortunately, we resolved it with an agreement which I think does address the principal concerns that we have. But it focused my attention on how much of my ability to do my job in leading a department that protects the American people depends upon constraints that others want to put upon us based on their conception of either international law or transnational law. So I've come to see in a very dramatic way, this has a real world impact on the fundamental issues about how we protect ourselves.

Of course, it turns out that this is not a new issue. If you go back in 1986, there was a case in the International Court of Justice called Nicaragua v. the United States where there was a challenge to the United States policy of supporting the contras. And the court there was confronted by a jurisdictional argument which the United States raised.

The argument was that, based on the various treaties which were enforced, which meant things that we and other countries had agreed to, the court didn't really have jurisdiction of the case because all of the relevant parties were not participating, but the court brushed that jurisdictional argument aside and ruled against the United States on the ground that even if the treaties did not permit this to be addressed in that particular forum, there was customary law that allowed the court to act even though the treaties would have forbidden action in that case. And that's a fairly significant and dramatic decision, at least in my view.

In 1998, the International Court of Justice again confronted the United States in Breard v. Gilmore. That involved a Paraguayan who had not been given access to his consul -- I think frankly because nobody knew he was Paraguayan -- in Virginia, had worked his way up and down the state system in Virginia -- after he was convicted and sentenced to death, was working his way up the federal system. And literally at the eleventh hour of his execution, Paraguay went into the International Court of Justice and ordered the United States not to complete the sentence that had been imposed by a duly constituted Virginia state court.

Ultimately, it went up to the U.S. Supreme Court. And the U.S. Supreme Court ruled that because the court -- the plaintiff Breard had not exhausted or raised these issues at any point in the state court proceedings, he had waived his rights. There was a procedural bar under a 1986 federal statute that basically said you've got to raise your claims in accordance with state law or you've waived them. And therefore the execution went ahead. But international lawyers in the international courts were outraged that we gave greater weight to a federal statute that came after the treaty in question rather than deferring to an international court.

And of course, it's not only been the United States that has felt the vigor of this -- what I would call very activist -- kind of international adjudication. In 2004, the International Court of Justice waded into a thicket that is probably one of the most difficult of all in the area of international relations, and that has to do with Israel and its activities in the West Bank of the Jordan River. There, in a case entitled Legal Consequences of Construction of a Wall in the Occupied Palestinian Territory, the ICJ issued a very broad advisory opinion concluding that the construction of a wall that was specifically designed to keep suicide bombers out of Israel, where they were blowing up people on a regular basis, violated international law, had to be dismantled, and reparations had to be made because the wall was put up.

Part of that reasoning process was the ICJ concluding that Israel could not use the threat of terrorist attacks emanating for the Palestinian territories to justify the wall because the attacks were not attributed to a state. In other words, using what I would consider a very hyper-technical reading, the court was relatively dismissive of what most of us would regard as a very compelling, fundamental attribute of state sovereignty -- the right to protect your citizens from being killed by people coming in from outside.

And I think this sequence of decisions shows an increasing tendency to look to rather generally described and often ambiguous "universal norms" to trump domestic prerogatives that are very much at the core of what it means to live up to your responsibility as a sovereign state. Now who interprets these laws? Of course, to the extent we're dealing with the text of treaties, if this country is party to a treaty we have consented to it -- if it's been ratified by the Senate -- and it's fair that we live up to the letter of the agreement we have signed.

But often the letter of the agreement is not what controls; it is, in fact, what we have not agreed to that people seek to impose upon us. And of course this begins with the judges and justices of various international courts, not, of course, appointed by or ratified by our legal -- our political process, that looks to customary international law, that is often considered to be described by what they say are the opinions of international law experts. That basically means professors.

Now I'm sure it's an academic fantasy to imagine a world in which the writings of professors actually define the content of the law rather than what Congress passes or is agreed upon. That's typically not, at least not in my experience, the way we make law in this country. But it is quite seriously the view taken by some that international law can be discovered in the writings of academics and others who are experts, often self-styled experts.

And I think Congress itself has recognized that this tendency to have a very expansive and activist view of customary international law requires that we be very cautious in this country about how we address the issue. Several times, for example, the Senate has expressly put reservations into its approval of treaties to make sure that the treaties are interpreted and applied domestically in a limited fashion, or even more importantly in a way that's consistent with our own fundamental constitutional requirements.

And yet again, the experts and sometimes the foreign adjudicators simply view those limitations as minor impediments to insistence that we accept the full measure of the treaty as ratified by others, or perhaps as not ratified by anybody, but as having its source in that vague and fertile turf of customary international law.

And of course, when one looks to the sources of this international law, one can hardly, for example, fail to note the composition of the U.N. Human Rights Committee and other U.N. organs which often take some of their impetus for their view of international from countries like Cuba and Zimbabwe, which are not notable upholders of the rule of law in their own countries.

And the increasing tendency of the U.N. and similar bodies to enter into the domestic arena with aggressive views of international law that would requires us, for example, to second-guess the Patriot Act, or to accord illegal immigrants in the United States equal rights with those who are here legally.

But perhaps even more urgently in the current arena, we see the impact of international and transnational law on our

struggle to defeat an enemy that wants to bring war to our shores and successfully did so on 9/11.

I've talked about the PNR, passenger name record, issue we've had with Europe, in which some in the European Parliament argued that the fact that the information was derived from Europeans coming to the U.S. meant that we should be forced in the United States to let Europe supervise and set the terms of how we make use of that information. A press report I saw today suggested a similar measure by some European privacy advocates to limit the way in which financial information that we gather can be used in our country, because at some point that information may have passed through European hands.

So how we deal with this issue of international law is increasingly impacting how we defend ourselves and how we conduct our domestic affairs. So what's the source of all this? Well, the source of it, I think, has to do with what I said at the very beginning of the speech. It's the fact that the concept of judicial modesty, which at least has won respect in this country, of not perhaps completely unanimous agreement, is, I think, pretty much absent in those areas where people develop and discuss international law. And if you look at the cases I've talked about, it illustrates the point very well.

A critical element of judicial modesty is deferring to the political and Democratic branches, to those who govern with the consent of the people. And even when we talked about overriding those with the Constitution, it's because our Constitution is a document which reflects the consent of the people. But in the Nicaragua case, the ICJ, International Court of Justice, precisely rejected consent by pushing to one side the carefully crafted treaty limitations about who should be present in the court before the court could rule, and then simply going ahead and reaching for customary law.

And recently a leading practitioner in the area of international human rights law was quite specific in saying that when the U.S. refuses to ratify a treaty, it doesn't matter, because we may still be bound by customary international law. Or in the Breard case, where the international law community gave short shrift to Congress's mandate that we respect the procedural rules and regulations of the state courts. In other words, a critical element of federalism, reflected not only in our Constitution but in a specific act of Congress, was viewed as an impediment to be brushed aside in the service of a more general and, frankly, somewhat vaguer set of international norms.

So what we see here is a vision of international law that if taken aggressively would literally strike at the heart of some of our basic fundamental principles: separation of power, respect for the Senate's ability to ratify treaties, and the Senate's ability to reject treaties, and respect for federalism and the importance of letting the state courts set their own rules to govern what they do.

So where is all this leading? Well, I'm going to quote from the same international human rights lawyer who gives us his vision of where we're going with international law. He says in a recent book called Lawless World, "to claim that states are as sovereign today as they were 50 years ago is to ignore reality. The extent of inter-dependence caused by the avalanche of international laws means that states are constrained by international obligations over an increasingly wide range of actions, and the rules, once adopted, take on a logic and a life of their own. They do not stay within the neat boundaries that states thought they were creating when they were negotiating."

Now, I'm quite sure that is meant to be a happy statement of the way we're operating now. But I actually view it as a chilling vision of where we could go, given the current developments in international and transnational law. So what do we do about it?

Well, traditionally, we have tended to act in a manner that I would call defensive. For example, after the Nicaragua case, the U.S. government withdrew jurisdiction over the matter and that ended the legal power of the International Court such as it was to compel a result.

In some of the more extravagant assertions by some of the U.N. human rights organs, we've simply accepted this statement as a kind of hortatory request, and we haven't done anything further with it.

And of course, those of you who fellow the developments with the International Criminal Court know that we have sought to enter agreements with other countries to avoid the application of that court's rules against our own citizens when we haven't, in fact, ratified or agreed to that treaty.

But while these defensive means may be necessary, they are not, in my view, a sufficient approach to this increasing challenge to our ability to conduct our domestic affairs.

First of all, the fact is whether we like it not, international law is increasingly entering our domestic domain. The Supreme Court has begun to bring it through cases like Hamdan and Alvarez-MacHain, which allowed a very small opening but still an opening in the door under the Alien Tort Claims Act to international human rights law being a source of direct causes of action here in the United States.

Through various European and other kinds of domestic protection rules, they're trying -- there's an increasing effort to control our use of information in our own country to determined who comes in from outside, and, of course, international law is being used as a rhetorical weapon against us. We are constantly portrayed as being on the losing end, and the negative end of international law developments.

And I also have to say in fairness there are some positive things that a properly constructed and implemented international law can do not only for the whole world but for us, as well. Common standards on aviation and maritime security are a win-win for us and for our allies overseas. There is a positive dimension to international law if we can recapture it from those elements that seem to make it into a kind of activism on steroids.

So my bottom line is this: The problem is not the idea of international law, but it is an international law that has been captured by a very activist, extremist legal philosophy. But it doesn't have to be that way. And so my challenge to you is to take overseas the same kind of intellectual vigor and intellectual argument that you brought into the United States and into academia in the United States in the '70s, and that was quite successful over a period of time in changing the playing field, leveling it out, so that there was another voice heard for judicial modesty.

I'm confident it's not going to happen in a week or a month or a year, but that if you take some of the ideas you've developed here, and you take them overseas and you take them to academia, and you take them into the legal-philosophical salons in Europe, you will eventually start to persuade because the merit of these ideas I think is strong. And what's wanting is the energy and the initiative and the courage to take them to a place where until now they have not been very seriously heard.

Thank you very much.

Question: Mr. Secretary, my question concerns no-fly lists. How do you get on a list? How do you get off a list? And why not give the American citizen his day in court to contest the proposed action of your department?

Secretary Chertoff: Well, if you want to get on the list, I think I probably can put you on.

The no-fly list -- the process, without getting into classified material, basically involves a determination that there's intelligence about someone being a threat to aviation. And based on that determination, we judge through an inter-agency process whether someone ought to be put on the no-fly list. And the list is then transmitted to the airlines and winds up then being a basis to deny people -- they're actually legally obliged to deny people the opportunity to fly.

People can -- if they have an issue with it, they can raise an issue with it. But we don't conduct court hearings on this. We don't believe first of all, almost all the information is classified; second, because I'm quite sure that the 19 hijackers, if we could replay history, would have contested being on a no-fly list, and we're not about to let them do that; and third, because we would be inundated with proceedings.

This is the kind of measure you have to undertake if you're going to protect the airlines from being blown up. Now, we do sometimes revisit these things. And if we have a basis to believe, for example, that a mistake has been made, we've taken people off the list. And sometimes for people who have refused -- been refused boarding, they will raise the issue. They'll write in, or they'll have somebody contact us. And we will consider if they've got some reason to believe that they shouldn't be on the list.

I should separate that from mistakes in identity. Those we always do correct. And the problem often arises with mistakes in identity that we actually have been prohibited from gathering some limited additional information that would actually allow us to separate people who have the same name from people that are really in danger. So I want to be clear that when we have mistakes, we correct those and we tell the airlines that they ought to be corrected.

But people who are -- when we actually have identified a person as the right person and we put them on the list, based on our careful consideration of intelligence, it's not a subject for litigation.

###

Exhibit E

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

November 7, 2006

BY FACSIMILE — (571) 227-1125

Catherine M. Papoi
Acting Director
Departmental Disclosure & FOIA
Department of Homeland Security
Arlington, VA 22202

RE: **Freedom of Information Act Request and Request for Expedited Processing**

Dear Ms. Papoi:

This letter constitutes an expedited request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the Department of Homeland Security ("DHS") on behalf of the Electronic Frontier Foundation ("EFF"). We make this request as part of EFF's FOIA Litigation for Accountable Government ("FLAG") Project, which works to obtain government documents and make them widely available to the public.

On November 2, 2006, DHS published a Privacy Act notice in the Federal Register concerning what it described as a "new system of records" identified as the Automated Targeting System ("ATS"). 71 FR 64543. According to the notice, "[t]he new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination." *Id.*

We are seeking the following agency records (including, but not limited to, electronic records) concerning the 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 ("CPB") and the Canada Border Services Agency to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information; and

3. all records, including Privacy Act notices, that discuss or describe the use of personally-identifiable information by CPB (or its predecessors) for purposes of "screening" air and sea travelers.[1]

[1] To assist you in searching for records responsive to this portion of our request, we note that an Associated Press article dated November 3 (attached hereto) quoted DHS spokesman Russ Knocke as saying that "screening for air and sea travelers has been in place since the 1990s."

1875 Connecticut Ave., NW · Suite 650 · Washington, DC 20009
202 797 9009 202 797 9066 www.eff.org information@eff.org

Request for Expedited Processing

This request warrants expedited processing because it 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." 6 CFR § 5.5(d)(1)(ii).

First, there is substantial public interest in the Department's use of the ATS to assign "risk assessments" to American citizens. A search conducted on Google News indicates that since the Federal Register notice was published five days ago, 58 articles have been published that discuss the system and the privacy issues it raises (see first page of search results, attached hereto). The published articles include coverage by the Washington Post and the Associated Press (see attached articles).

Further, there is an "urgency to inform the public" about the potential privacy implications of the ATS because the Department has solicited public comments and announced that "[t]he new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination." 71 FR 64543. Indeed, it is difficult to imagine circumstances where there would be a greater "urgency to inform the public" than when an agency has solicited public comment on a significant issue, set a short deadline for the submission of comments, and stated its intention to go forward with its proposal "unless comments are received that result in a contrary determination."

The purpose of this request is to obtain information directly relevant to DHS's Privacy Act notice and the practices it describes (which will affect tens of millions of American citizens). 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 on the issue prior to the December 4 deadline the Department has imposed.

Further, as I explain below in support of our request for "news media" treatment, EFF is "primarily engaged in disseminating information."

Request for News Media Fee Status

EFF asks that it not be charged search or review fees for this request because EFF qualifies as a representative of the news media pursuant to the FOIA and 6 C.F.R. § 5.11(b)(6).

EFF is a non-profit public interest organization that works "to protect and enhance our core civil liberties in the digital age."[2] One of EFF's primary objectives is "to educate the press, policymakers and the general public about online civil liberties."[3] To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

---

[2] Guidestar Basic Report, Electronic Frontier Foundation, http://www.guidestar.org/pqShowGsReport.do?npoId=561625 (last visited Oct. 16, 2006).
[3] *Id.*

First, EFF maintains a frequently visited web site, http://www.eff.org, which received 40,681,430 hits in September 2006 — an average of 56,501 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.

EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 77,000 subscribers. A complete archive of past EFFectors is available at http://www.eff.org/effector/.

Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (http://www.eff.org/deeplinks/) reports and analyzes newsworthy developments in technology. It also provides miniLinks, which direct readers to other news articles and commentary on these issues. DeepLinks had 538,297 hits in September 2006.[4]

In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than eighteen white papers published since 2002. These papers, available at http://www.eff.org/wp/, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.

EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (http://www.powells.com). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (http://www.amazon.com). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at http://cryptome.org/cracking-des.htm and for sale at Amazon.com.

Most recently, EFF has begun broadcasting podcasts of interviews with EFF staff and outside experts. *Line Noise* is a five-minute audio broadcast on EFF's current work, pending legislation, and technology-related issues. A listing of *Line Noise* podcasts is available at feed://www.eff.org/rss/linenoisemp3.xml and feed://www.eff.org/rss/linenoiseogg.xml. These podcasts were downloaded more than 1,300 times from EFF's web site last month.

Request for a Public Interest Fee Waiver

EFF is entitled to a waiver of duplication fees because disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(a)(iii) and 6 C.F.R. § 5.11(k). To determine whether a request meets this standard, Department of Homeland Security components determine whether "[d]isclosure of the requested information is likely to contribute

[4] These figures include hits from RSS feeds through which subscribers can easily track updates to DeepLinks and miniLinks.

significantly to public understanding of the operations or activities of the government," and whether such disclosure "is not primarily in the commercial interest of the requester." 6 C.F.R. §§ 5.11(k)(i), (ii). This request clearly satisfies these criteria.

First, DHS's handling of personal data and the assignment of "risk assessments" concern "the operations or activities of the government." 6 C.F.R. § 5.11(k)(2)(i). DHS is a government agency, and its use of passenger data to make determinations about travelers unquestionably constitutes government operations or activities.

Second, disclosure of the requested information will "contribute to an understanding of government operations or activities." 6 C.F.R. § 5.11(k)(2)(ii) (internal quotation marks omitted). EFF has requested information that will shed light on the manner in which DHS uses personal data to screen travelers entering or exiting the United States, as well as the subsequent retention, uses, and disclosures of that data.

Third, the requested material will "contribute to public understanding" of DHS's handling of personal data. 6 C.F.R. § 5.11(k)(2)(iii) (internal quotation marks omitted). This information will contribute not only to EFF's understanding of DHS's data privacy policies, but to the understanding of a reasonably broad audience of persons interested in the subject. EFF will make the information it obtains under the FOIA available to the public and the media through its web site and newsletter, which highlight developments concerning privacy and civil liberties issues, and/or other channels discussed more fully above.

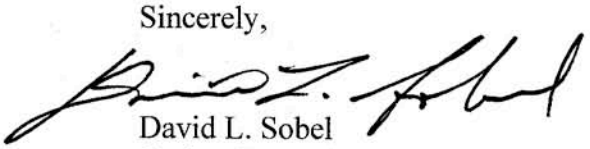
Fourth, the disclosure will "contribute significantly" to the public's knowledge and understanding of how DHS handles personal data. 6 C.F.R. § 5.11(k)(2)(iv) (internal quotation marks omitted). Disclosure of the requested information will help inform the public about the contours of the ATS process, as well as contribute to the public debate about the adequacy of the privacy policies surrounding the system.

Furthermore, a fee waiver is appropriate here because EFF has no commercial interest in the disclosure of the requested records. 6 C.F.R. § 5.11(k)(3). EFF is a 501(c)(3) nonprofit organization, and will derive no commercial benefit from the information at issue here.

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact me at (202) 797-9009 x. 10. As the FOIA provides, I will anticipate a determination on our expedition request within 10 calendar days.

Under penalty of perjury, I hereby affirm that the foregoing is true and correct to the best of my knowledge.

Sincerely,



David L. Sobel
Senior Counsel

Sign in

Google News

Web Images Video **News** Maps **more »**

"automated targeting system" Search News Search the Web Advanced news search Preferences

Results **1** - **58** of **58** for **automated-targeting-system**. (**0.18** seconds)

Sort by relevance **Sorted 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

DHS Plans To Screen All Who Enter, Leave US
Officer.com - 1 hour ago
... The department intends to use a program called the **Automated Targeting System**, originally designed to screen shipping cargo, to store and analyze the data. ...

Border screening details released
Wilmington Morning Star, NC - 8 hours ago
... Knocke. The notice provides details of the **Automated Targeting System**, which, it said, processes and stores information on travelers.

US Plans to Screen All Who Enter, Leave Country
Infoshop News - 22 hours ago
... The department intends to use a program called the **Automated Targeting System**, originally designed to screen shipping cargo, to store and analyze the data. ...

Homeland Security data mining all international travelers
Homeland Stupidity (satire), DC - Nov 5, 2006
... The **Automated Targeting System** has been used for many years to develop risk assessments for each piece of cargo coming in to the US But it was only after 9/11 ...

Government releases details on border screening
Helena Independent Record, MT - Nov 4, 2006
... The notice provides details of the **Automated Targeting System**, which in the past was used primarily to help identify and inspect US-bound cargo. ...

Govt. Gives Details on Border Screening
Wyoming News, WY - Nov 4, 2006
... The notice provides details of the **Automated Targeting System**, which in the past was used primarily to help identify and inspect US-bound cargo. ...

Border screening data being compiled
Daily Breeze, CA - Nov 4, 2006

washingtonpost.com

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

By Ellen Nakashima and Spencer S. Hsu
Washington Post Staff Writers
Friday, November 3, 2006; A18

The federal government disclosed details yesterday of a border-security program to screen all people who enter and leave the United States, create a terrorism risk profile of each individual and retain that information for up to 40 years.

The details, released in a notice published yesterday in the Federal Register, open a new window on the government's broad and often controversial data-collection effort directed at American and foreign travelers, which was implemented after the Sept. 11, 2001, attacks.

While long known to scrutinize air travelers, the Department of Homeland Security is seeking to apply new technology to perform similar checks on people who enter or leave the country "by automobile or on foot," the notice said.

The department intends to use a program called the Automated Targeting System, originally designed to screen shipping cargo, to store and analyze the data.

"We have been doing risk assessments of cargo and passengers coming into and out of the U.S.," DHS spokesman Jarrod Agen said. "We have the authority and the ability to do it for passengers coming by land and sea."

In practice, he said, the government has not conducted risk assessments on travelers at land crossings for logistical reasons.

"We gather, collect information that is needed to protect the borders," Agen said. "We store the information we see as pertinent to keeping Americans safe."

Civil libertarians expressed concern that risk profiling on such a scale would be intrusive and would not adequately protect citizens' privacy rights, issues similar to those that have surrounded systems profiling air passengers.

"They are assigning a suspicion level to millions of law-abiding citizens," said David Sobel, senior counsel of the Electronic Frontier Foundation. "This is about as Kafkaesque as you can get."

DHS officials said that by publishing the notice, they are simply providing "expanded notice and transparency" about an existing program disclosed in October 2001, the Treasury Enforcement

Communications System.

But others said Congress has been unaware of the potential of the Automated Targeting System to assess non-aviation travelers.

"ATS started as a tool to prevent the entry of drugs with cargo into the U.S.," said one aide, who spoke on the condition of anonymity because of the sensitivity of the subject. "We are not aware of Congress specifically legislating to make this expansion possible."

The Senate Homeland Security and Governmental Affairs Committee, chaired by Sen. Susan Collins (R-Maine), yesterday asked Homeland Security to brief staff members on the program, Collins's spokeswoman, Jen Burita, said.

The notice comes as the department is tightening its ability to identify people at the borders. At the end of the year, for example, Homeland Security is expanding its Visitor and Immigrant Status Indicator Technology program, under which 32 million noncitizens entering the country annually are fingerprinted and photographed at 115 airports, 15 seaports and 154 land ports.

Stephen E. Flynn, senior fellow for national security studies at the Council on Foreign Relations, expressed doubts about the department's ability to conduct risk assessments of individuals on a wide scale.

He said customs investigators are so focused on finding drugs and weapons of mass destruction that it would be difficult to screen all individual border crossers, other than cargo-truck drivers and shipping crews.

"There is an ability in theory for government to cast a wider net," he said. "The reality of it is customs is barely able to manage the data they have."

The data-mining program stemmed from an effort in the early 1990s by customs officials to begin assessing the risk of cargo originating in certain countries and from certain shippers. Risk assessment turned more heavily to automated, computer-driven systems after the 2001 attacks.

The risk assessment is created by analysts at the National Targeting Center, a high-tech facility opened in November 2001 and now run by Customs and Border Protection.

In a round-the-clock operation, targeters match names against terrorist watch lists and a host of other data to determine whether a person's background or behavior indicates a terrorist threat, a risk to border security or the potential for illegal activity. They also assess cargo.

Each traveler assessed by the center is assigned a numeric score: The higher the score, the higher the risk. A certain number of points send the traveler back for a full interview.

The Automated Targeting System relies on government databases that include law enforcement data, shipping manifests, travel itineraries and airline passenger data, such as names, addresses, credit card details and phone numbers.

The parent program, Treasury Enforcement Communications System, houses "every possible type of information from a variety of federal, state and local sources," according to a 2001 Federal Register notice.

It includes arrest records, physical descriptions and "wanted" notices. The 5.3 billion-record database was

accessed 766 million times a day to process 475 million travelers, according to a 2003 Transportation Research Board study.

In yesterday's Federal Register notice, Homeland Security said it will keep people's risk profiles for up to 40 years "to cover the potentially active lifespan of individuals associated with terrorism or other criminal activities," and because "the risk assessment for individuals who are deemed low risk will be relevant if their risk profile changes in the future, for example, if terrorist associations are identified."

DHS will keep a "pointer or reference" to the underlying records that resulted in the profile.

The DHS notice specified that the Automated Targeting System does not call for any new means of collecting information but rather for the use of existing systems. The notice did not spell out what will determine whether someone is high risk.

But documents and former officials say the system relies on hundreds of "rules" to factor a score for each individual, vehicle or piece of cargo.

According to yesterday's notice, the program is exempt from certain requirements of the Privacy Act of 1974 that allow, for instance, people to access records to determine "if the system contains a record pertaining to a particular individual" and "for the purpose of contesting the content of the record."

USA TODAY

Government releases details on border screening

Posted 11/3/2006 3:02 PM ET

WASHINGTON (AP) — Every person entering or leaving the country could be subject to data collection and risk assessment under the border security program outlined in a federal document.

The Federal Register, in a report published Thursday, also said data collected on travelers can be retained for up to 40 years.

The Department of Homeland Security on Friday stressed that the border monitoring outlined in the notice was not a new program or an expansion of an existing program. "There is nothing new here," said Homeland Security spokesman Russ Knocke. "All that is new is that the department is fulfilling the spirit of the Privacy Act by updating the federal record."

The notice provides details of the Automated Targeting System, which in the past was used primarily to help identify and inspect U.S.-bound cargo. The system, it said, processes and stores information on air and sea travelers, as well as those arriving by automobile or foot.

It said the system builds a risk assessment for cargo, conveyance and travelers based on criteria developed by the Bureau of Customs and Border Protection.

For air and sea passengers, it maintains information provided by the commercial carrier, such as payment information, billing addresses, contact telephone numbers and e-mail addresses.

Knocke said screening for air and sea travelers has been in place since the 1990s and the Federal Register notice was part of an effort to provide transparency on an existing program as the newly created Homeland Security Department takes over programs previously under the jurisdiction of the Treasury Department.

The department has a parallel program, the Visitor and Immigration Status Indicator Technology program, or US-VISIT, that uses biometric technology, including fingerprinting to screen visitors. The program has been deployed to 116 airports, 15 seaports and 154 land ports of entry and processed more than 61 million people applying for admission to the country.

Find this article at:
http://www.usatoday.com/news/washington/2006-11-03-screening_x.htm

Exhibit F
(Part 1)

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Electronic Frontier Foundation
Protecting Rights and Promoting Freedom on the Electronic Frontier

December 6, 2006

BY FACSIMILE — (571) 227-1125

Catherine M. Papoi
Acting Director
Departmental Disclosure & FOIA
Department of Homeland Security
Arlington, VA 22202

RE: **Freedom of Information Act Request and Request for Expedited Processing**

Dear Ms. Papoi:

This letter constitutes an expedited request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted to the Department of Homeland Security ("DHS") on behalf of the Electronic Frontier Foundation ("EFF"). We make this request as part of EFF's FOIA Litigation for Accountable Government ("FLAG") Project, which works to obtain government documents and make them widely available to the public.

On November 2, 2006, DHS published a Privacy Act notice in the Federal Register concerning what it described as a "new system of records" identified as the Automated Targeting System ("ATS"). 71 FR 64543. According to the notice, "[t]he new system of records will be effective December 4, 2006, unless comments are received that result in a contrary determination." *Id.* According to a Department spokesman, since "the mid-1990s, [ATS] was being used to screen airline passengers and has expanded in use by Homeland Security since the department was created almost four years ago." Exhibit 1 (attached hereto). As noted below, DHS yesterday extended the public comment period until December 29.

We are seeking the following agency records (including, but not limited to, electronic records) concerning the ATS:

1. all Privacy Impact Assessments prepared for the ATS or any predecessor system that served the same function but bore a different name;

2. all System of Records Notices ("SORNs") that discuss or describe targeting, screening or assigning "risk assessments" of U.S. citizens by Customs and Border Protection (or its predecessors);

3. all records that discuss or describe the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them;

1875 Connecticut Ave., NW · Suite 650 · Washington, DC 20009
202 797 9009 202 797 9066 www.eff.org information@eff.org

4. all records that discuss or describe the potential consequences that individuals might experience as a result of the agency's use of the ATS, including but not limited to arrest, physical searches, surveillance, denial of the opportunity to travel, and loss of employment opportunities;

5. 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;

6. all complaints received from individuals concerning actions taken by the agency as a result of ATS "risk assessments" or other information contained in the ATS, and the agency's responses to those complaints;

7. all records that discuss or describe Section 514 of the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441) and its prohibition against the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists;" and

8. all records that address any of the following issues:

a) whether a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights may appeal such decision and correct erroneous information contained in the ATS;

b) whether the underlying error rate of the government and private data bases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;

c) whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;

d) whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;

e) whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;

f) whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;

g) whether the agency has adopted policies establishing effective oversight of the use and operation of the system;

h) whether there are no specific privacy concerns with the technological architecture of the system;

i) whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate States with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and

j) whether appropriate life-cycle cost estimates, and expenditure and program plans exist.

Request for Expedited Processing

This request warrants expedited processing because it 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." 6 CFR § 5.5(d)(1)(ii).

First, there is substantial public interest in the Department's use of the ATS to assign "risk assessments" to American citizens. A search conducted on Google News indicates that since the Federal Register notice was published on November 2, almost 900 articles have been published that discuss the system and the privacy issues it raises (see first page of search results, attached hereto as Exhibit 2). The published articles include coverage by the Washington Post and the Associated Press (see Exhibits 3 & 4).

Further, there is an "urgency to inform the public" about the potential privacy implications of the ATS because the Department has solicited public comments and yesterday extended the comment period until December 29. In addition, Sen Patrick Leahy, incoming chairman of the Senate Judiciary Committee, has announced that oversight of the ATS and similar systems will occur when the new Congress convenes in January. Exhibits 1 & 5. Similarly, Senate Homeland Security Investigations Subcommittee Chairman Norm Coleman has indicated he also is examining the system. Sen. Coleman said, "We must ensure that this program is indeed working to prevent terrorism, while at the same time safeguarding the privacy of air travelers." Exhibit 1. Rep. Bennie Thompson, incoming chairman of the House Homeland Security Committee has written in a letter to Secretary Chertoff that "serious concerns have arisen that . . . some elements of ATS as practiced may constitute violations of privacy or civil rights." Exhibit 6.

The purpose of this request is to obtain information directly relevant to DHS's Privacy Act notice and the practices it describes (which will affect tens of millions of American citizens). 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, and prior to the Congressional consideration of the system when the new Congress convenes in January.

Further, as I explain below in support of our request for "news media" treatment, EFF is "primarily engaged in disseminating information."

Request for News Media Fee Status

EFF asks that it not be charged search or review fees for this request because EFF qualifies as a representative of the news media pursuant to the FOIA and 6 C.F.R. § 5.11(b)(6).

As an initial matter, I note that the Department recently acknowledged that EFF qualifies for "news media" fee status. In a letter to my colleague Marcia Hofmann, dated November 17, 2006, the Department informed us that "[f]or purposes of fees, your organization is considered news media," and that EFF is subject to fees "for duplication only." Exhibit 7. The agency's recent determination of our fee status was based upon the information reiterated below, which remains accurate and up-to-date.

EFF is a non-profit public interest organization that works "to protect and enhance our core civil liberties in the digital age."[1] One of EFF's primary objectives is "to educate the press, policymakers and the general public about online civil liberties."[2] To accomplish this goal, EFF routinely and systematically disseminates information in several ways.

First, EFF maintains a frequently visited web site, http://www.eff.org, which received 40,681,430 hits in September 2006 — an average of 56,501 per hour. The web site reports the latest developments and contains in-depth information about a variety of civil liberties and intellectual property issues.

EFF has regularly published an online newsletter, the EFFector, since 1990. The EFFector currently has more than 77,000 subscribers. A complete archive of past EFFectors is available at http://www.eff.org/effector/.

Furthermore, EFF publishes a blog that highlights the latest news from around the Internet. DeepLinks (http://www.eff.org/deeplinks/) reports and analyzes newsworthy developments in technology. It also provides miniLinks, which direct readers to other news articles and commentary on these issues. DeepLinks had 538,297 hits in September 2006.[3]

In addition to reporting hi-tech developments, EFF staff members have presented research and in-depth analysis on technology issues in no fewer than eighteen white papers published since 2002. These papers, available at http://www.eff.org/wp/, provide information and commentary on such diverse issues as electronic voting, free speech, privacy and intellectual property.

---

[1] Guidestar Basic Report, Electronic Frontier Foundation, http://www.guidestar.org/pqShowGsReport.do?npoId=561625 (last visited Oct. 16, 2006).

[2] *Id.*

[3] These figures include hits from RSS feeds through which subscribers can easily track updates to DeepLinks and miniLinks.

EFF has also published several books to educate the public about technology and civil liberties issues. *Everybody's Guide to the Internet* (MIT Press 1994), first published electronically as *The Big Dummy's Guide to the Internet* in 1993, was translated into several languages, and is still sold by Powell's Books (http://www.powells.com). EFF also produced *Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace* (HarperEdge 1998), a "comprehensive guide to self-protection in the electronic frontier," which can be purchased via Amazon.com (http://www.amazon.com). Finally, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (O'Reilly 1998) revealed technical details on encryption security to the public. The book is available online at http://cryptome.org/cracking-des.htm and for sale at Amazon.com.

Most recently, EFF has begun broadcasting podcasts of interviews with EFF staff and outside experts. *Line Noise* is a five-minute audio broadcast on EFF's current work, pending legislation, and technology-related issues. A listing of *Line Noise* podcasts is available at feed://www.eff.org/rss/linenoisemp3.xml and feed://www.eff.org/rss/linenoiseogg.xml. These podcasts were downloaded more than 1,300 times from EFF's web site last month.

Request for a Public Interest Fee Waiver

EFF is entitled to a waiver of duplication fees because disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(a)(iii) and 6 C.F.R. § 5.11(k). To determine whether a request meets this standard, Department of Homeland Security components determine whether "[d]isclosure of the requested information is likely to contribute significantly to public understanding of the operations or activities of the government," and whether such disclosure "is not primarily in the commercial interest of the requester." 6 C.F.R. §§ 5.11(k)(i), (ii). This request clearly satisfies these criteria.

First, DHS's handling of personal data and the assignment of "risk assessments" concern "the operations or activities of the government." 6 C.F.R. § 5.11(k)(2)(i). DHS is a government agency, and its use of passenger data to make determinations about travelers unquestionably constitutes government operations or activities.

Second, disclosure of the requested information will "contribute to an understanding of government operations or activities." 6 C.F.R. § 5.11(k)(2)(ii) (internal quotation marks omitted). EFF has requested information that will shed light on the manner in which DHS uses personal data to screen travelers entering or exiting the United States, as well as the subsequent retention, uses, and disclosures of that data.

Third, the requested material will "contribute to public understanding" of DHS's handling of personal data. 6 C.F.R. § 5.11(k)(2)(iii) (internal quotation marks omitted). This information will contribute not only to EFF's understanding of DHS's data privacy policies, but to the understanding of a reasonably broad audience of persons interested in the subject. EFF will make the information it obtains under the FOIA available to the public and the media through its web site and newsletter, which highlight developments concerning privacy and civil liberties issues, and/or other channels discussed more fully above.

Fourth, the disclosure will "contribute significantly" to the public's knowledge and understanding of how DHS handles personal data. 6 C.F.R. § 5.11(k)(2)(iv) (internal quotation marks omitted). Disclosure of the requested information will help inform the public about the contours of the ATS process, as well as contribute to the public debate about the adequacy of the privacy policies surrounding the system.

Furthermore, a fee waiver is appropriate here because EFF has no commercial interest in the disclosure of the requested records. 6 C.F.R. § 5.11(k)(3). EFF is a 501(c)(3) nonprofit organization, and will derive no commercial benefit from the information at issue here.

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact me at (202) 797-9009 x. 10. As the FOIA provides, I will anticipate a determination on our expedition request within **10 calendar days**.

Under penalty of perjury, I hereby affirm that the foregoing is true and correct to the best of my knowledge.

Sincerely,

David Sobel

David L. Sobel
Senior Counsel

attachments

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 1

GOVEXEC.COM
DAILY BRIEFING
December 4, 2006

Traveler screening to continue despite public outcry

By Chris Strohm, National Journal's Technology Daily

The Homeland Security Department plans to continue using a controversial program to screen all travelers to and from the United States, despite mounting calls that the program be suspended until Congress and the public have more time to investigate it.

Homeland Security spokesman Jarrod Agen on Monday said the department will not suspend its use of the Automated Targeting System, which aggregates information on people traveling to and from the United States by land, air and sea, including U.S. citizens.

The program assigns terror risk scores to people identified as posing a threat to U.S. national security. Records on travelers can be kept for 40 years. The program was originally developed by the Customs Service to screen cargo in the 1990s.

But by the mid-1990s, it also was being used to screen airline passengers and has expanded in use by Homeland Security since the department was created almost four years ago, Agen said.

"What is expected of the department is to be able to use data that is collected," he said. "It is the department's job to ascertain if there is a high risk from cargo or a traveler headed to the United States to protect us from an attack."

Last month, the department posted a notice giving the public until Monday to comment on the system. "The notice was put out so that the public was aware of the screening procedures that the department has," Agen said.

Almost 50 comments had been received from individuals and organizations by this afternoon, the majority of which expressed opposition to the program.

Critics include former Rep. Bob Barr, R-Ga., who runs the consulting firm Liberty Strategies. He said the program "not only constitutes a highly intrusive and unconstitutional evidence-gathering system on law-abiding citizens, but it is neither an effective nor cost-efficient way to identify terrorists attempting to use the airlines to carry out terrorist acts. It should be scrapped."

Patrick Leahy, D-Vt., plans to examine the program when he takes over the Senate Judiciary Committee in January, according to an aide. "New technologies make data banks more powerful and more useful than they have ever been before," Leahy said. "They have a place in our security regimen. But powerful tools like this are easy to abuse and are prone to mistakes."

Senate Homeland Security Investigations Subcommittee Chairman Norm Coleman, R-Minn., said he also is examining the program. The subcommittee is assessing the tool for air passengers and U.S.-bound cargo, he said. "We must ensure that this program is indeed working to prevent terrorism, while at the same time safeguarding the privacy of air travelers."

Diverse groups from the American Civil Liberties Union to the Business Travel Coalition, a group that advocates on behalf of corporate travelers, said the program should be abandoned.

Department observers and privacy watchdogs "were stunned to learn of [the department's] intentions to near-secretly implement such a massively intrusive program behind the backs of Congress and the public," the Business Travel Coalition wrote.

This document is located at http://www.govexec.com/dailyfed/1206/120406tdpm1.htm

---

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 2

Sign in

Google News

Web Images Video **News** Maps **more »**

"automated targeting system" privacy | Search News | Search the Web | Advanced news search | Preferences

Results **1** - **100** of about **887** for **automated-targeting-system privacy**. (**0.23** seconds)

Top Stories
World
U.S.
Business
Sci/Tech
Sports
Entertainment
Health
Most Popular

News Alerts

RSS | Atom
About Feeds

Mobile News

About
Google News

Sort by relevance **Sorted by date**

DHS Extends Comment Period For Int'l Passenger Screening System
Business Travel News, NY - 1 hour ago
... is postponing its comment period deadline for the **Automated Targeting System** until Dec. 29, following pressure from trade groups, **privacy** advocates and ...

Snoops dog us
Brattleboro Reformer, United States - 10 hours ago
... One program overdue for scrutiny is the **Automated Targeting System**, or ATS. ... widespread surveillance of our daily lives without proper safeguards for **privacy**.". ...

Privacy advocates push for investigation, oversight of Bush ...
Raw Story, MA - 12 hours ago
... The chairperson of another **privacy** watchdog said that the recent revelation of the government's **Automated Targeting System** indicates that its use of "watch ...

US Government's secret terrorist scores
The Age, Australia - 16 hours ago
... Some **privacy** advocates call it one of the most intrusive and risky ... or land is scored by the Homeland Security Department's **Automated Targeting System**, or ATS. ...

Privacy watchdogs urge probe of spying program
GovExec.com - 18 hours ago
... Last week's revelation of the so-called **Automated Targeting System**, which rates passengers ... democracy is at risk when unprecedented threats to **privacy** and civil ...

DHS allows more time for input on traveler screening program
GovExec.com - 18 hours ago
... to make the public aware of the screening procedures used in the **Automated Targeting System**. ... of ATS as practiced may constitute violations of **privacy** or civil ...

US Government's secret terrorist scores
Sydney Morning Herald, Australia - 19 hours ago
... Some **privacy** advocates call it one of the most intrusive and risky ...

Exhibit F
(Part 2)

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 3

ACLU Urges U.S. to Stop Collection of Traveler Data

By Ellen Nakashima
Washington Post Staff Writer
Saturday, December 2, 2006; A05

Privacy advocates yesterday called on the federal government to scrap a Department of Homeland Security data-mining program designed to create terrorism risk assessments for every traveler who enters or leaves the United States.

The Automated Targeting System began as a means of screening cargo but was quietly expanded in recent years to screen and create risk profiles that will be retained for 40 years, The Washington Post reported last month after a notice describing the system appeared in the Federal Register.

The government has been scrutinizing air passengers for risks for 10 years, and assessments of some land border crossers have been conducted for about two years, a Customs and Border Protection official said in an interview Thursday.

The risk profiles, which single out travelers for extra attention from customs officials, were disclosed publicly for the first time in the Nov. 2 notice, raising concerns among privacy advocates.

In formal comments filed Friday with the Department of Homeland Security, of which the customs agency is a part, the ACLU urged the government to abandon the program.

"How come we never heard about it before?" said Barry Steinhardt, director of the ACLU's Technology and Liberty Project. "The fact that they've been doing it for 10 years, under what authority?"

David Sobel, senior counsel for the Electronic Frontier Foundation, said he believes the program's existence without notice violates the 1974 Privacy Act. He, too, opposes the program.

"I don't see the logic of collecting massive amounts of information on millions of innocent citizens in the name of locating a small number of suspected terrorists," he said. "Casting that large a net raises issues both with respect to the security benefits as well as the privacy impact of the system."

Customs officials expressed exasperation with the call to abandon the program.

"How do they expect us to determine who's safe and who's at risk?" asked Patrick Jones, an agency spokesman. "We have over one million people coming into the country every day, and our job is to protect the American public from people who might want to harm the American public."

A separate proposal to conduct risk assessments on air passengers, called CAPPS II, raised so much controversy in 2004 that it was derailed, and a successor program has stalled.

Jayson P. Ahern, a Customs and Border Protection assistant commissioner, said the agency intends to eventually enter data for all border crossers in the ATS database. The data include name, date of birth, flight itineraries and credit card information. It also can include a customs inspector's interview notes on a traveler.

Ahern said travelers are screened for risk based on "assumptions" that he would not disclose. Those deemed potentially risky would be flagged for follow-up, he said. The system does not assign a numeric score or color code, he said.

"When you look at all the [risk] factors, it just kicks it out that this person is a target for follow-up," Ahern said. In other words, he said, "somebody's targeted or not."

Government officials asserted that creating a vast database over time on travelers -- including those who are law-abiding -- will help analysts build models of normal and suspicious behavior. Ahern said 309 million land and sea border crossings and 87 million air border crossings are made each year. More than 95 percent are for lawful reasons, he said.

Staff writer Spencer S. Hsu and staff researcher Madonna Lebling contributed to this report.

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 4

YAHOO! NEWS

Back to Story - Help

Massive terror screening draws outrage

Associated Press

By MICHAEL J. SNIFFEN, Associated Press Writer
Fri Dec 1, 10:57 PM ET

A leader of the new Democratic Congress, business travelers and privacy advocates expressed outrage Friday over the unannounced assignment of terrorism risk assessments to American international travelers by a computerized system managed from an unmarked, two-story brick building in Northern Virginia.

Incoming Senate Judiciary Chairman Sen. Patrick Leahy (news, bio, voting record) of Vermont pledged greater scrutiny of such government database-mining projects after reading that during the past four years millions of Americans have been evaluated without their knowledge to assess the risks that they are terrorists or criminals.

"Data banks like this are overdue for oversight," said Leahy, who will take over Judiciary in January. "That is going to change in the new Congress."

The Associated Press reported Thursday that Americans and foreigners crossing U.S. borders since 2002 have been assessed by the Homeland Security Department's computerized Automated Targeting System, or ATS.

The travelers are not allowed to see or directly challenge these risk assessments, which the government intends to keep on file for 40 years. Some or all data in the system can be shared with state, local and foreign governments for use in hiring, contracting and licensing decisions. Courts and even some private contractors can obtain some of the data under certain circumstances.

"It is simply incredible that the Bush administration is willing to share this sensitive information with foreign governments and even private employers, while refusing to allow U.S. citizens to see or challenge their own terror scores," Leahy said. This system "highlights the danger of government use of technology to conduct widespread surveillance of our daily lives without proper safeguards for privacy."

The concerns spread beyond Congress.

"I have never seen anything as egregious as this," said Kevin Mitchell, president of the Business Travel Coalition, which advocates for business travelers. It's "evidence of what can happen when there isn't proper oversight and accountability."

By late Friday, the government had received 22 written public comments about its after-the-fact disclosure of the program last month in the Federal Register, a fine-print compendium of federal rules. All either opposed it outright or objected to the lack of a direct means for people to correct any errors in the database about themselves.

"As a U.S. citizen who spends much time outside the U.S., I can understand the need for good security," wrote one who identified himself as Colin Edmunds. "However, just as I would not participate in a banking/credit card system where I have no recourse to correct or even view my personal data, I cannot accept the same of my government."

Privacy advocates also were alarmed.

"Never before in American history has our government gotten into the business of creating mass `risk assessment' ratings of its own citizens," said Barry Steinhardt, a lawyer for the American Civil Liberties Union. "We are stunned" the program has been undertaken "with virtually no opportunity for the public to evaluate or comment on it."

The Homeland Security Department says the nation's ability to spot criminals and other security threats "would be critically impaired without access to this data."

And on Friday as the normal daily flow of a million or more people entered the United States by air, sea and land, the ATS program's computers continued their silent scrutiny. At that Virginia building with no sign, the managers of the National Targeting Center allowed an Associated Press photographer to briefly roam their work space.

But he couldn't reveal the building's exact location. None of the dozens of workers under the bright fluorescent lights could be named. Some could not be photographed.

The only clue he might have entered a government building was a montage of photos in the reception area of President Bush's visit to the center. But there was only one guard and a sign-in book.

Inside, red digital clocks on the walls showed the time in Istanbul, Baghdad, Islamabad, Bangkok, Singapore, Tokyo, and Sydney. Although billboard-size video screens on the walls showed multiple cable news shows, there was little noise in the basketball-court-sized main workroom. Each desk had dual computer screens and earphones to hear the video soundtrack. Conferences were held in smaller workrooms divided by glass walls from the windowless main room.

Round the clock, the targeters from Homeland Security's Customs and Border Protection agency analyze information from multiple sources, not just ATS. They compare names to terrorist watch lists and mine the Treasury Enforcement Communications System and other automated systems that bring data about cargo, travelers and commercial workers entering or leaving the 317 U.S. ports, searching for suspicious people and cargo.

Almost every person entering and leaving the United States by air, sea or land is assessed based on ATS' analysis of their travel records and other data, including items such as where they are from, how they paid for tickets, their motor vehicle records, past one-way travel, seating preference and what kind of meal they ordered.

Government officials could not say whether ATS has apprehended any terrorists. Based on all the information available to them, federal agents turn back about 45 foreign criminals a day at U.S. borders, according to Homeland Security's Customs and Border Protection spokesman Bill Anthony. He could not say how many were spotted by ATS.

Officials described how the system works: applying rules learned from experience with the activities and characteristics of terrorists and criminals to the traveler data. But they would not describe in detail the format in which border agents see the results or in which the databases store the results of the ATS risk assessments.

Acting Assistant Homeland Security Secretary Paul Rosenzweig told reporters Friday they could call it scoring. "It can be reduced to a number," he said, but he clearly preferred the longer description about how the rules are used.

On the Net:

DHS privacy impact statement: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats.pdf

Associated Press writers Leslie Miller and Beverley Lumpkin contributed to this report.

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 5

U.S. SENATOR PATRICK LEAHY

CONTACT: Office of Senator Leahy, 202-224-4242 **VERMONT**

Reaction Of Senator Patrick Leahy (D-Vt.), Ranking Member And Incoming Chairman, Senate Judiciary Committee, To Report That The Government Is Assigning Terror Scores To Travelers
Friday, December 1, 2006

"The recent revelation that, since 9/11, the U.S. government has been assigning terror scores to millions of law-abiding Americans who travel across our borders, without their knowledge, highlights the danger of government use of technology to conduct widespread surveillance of our daily lives without proper safeguards for privacy. It is simply incredible that the Bush Administration is willing to share this sensitive information with foreign governments and even private employers, while refusing to allow U.S. citizens to see or challenge their own terror scores.

"When done poorly or without proper safeguards and oversight, data banks do not make us safer, they just further erode Americans' privacy and civil liberties. This is an Administration that goes to unprecedented lengths to hide its own activities from the public, while at the same time collecting and compiling unprecedented amounts of information about every citizen.

"New technologies make data banks more powerful and more useful than they have ever been before. They have a place in our security regimen. But powerful tools like this are easy to abuse and are prone to mistakes. A mistake can cost Americans their jobs and wreak havoc in their lives. Mistakes on government watch lists have become legendary in recent years. We need checks and balances to keep government data bases from being misused against the American people.

"Data banks like this are overdue for oversight, and that is going to change in the new Congress."

#####

Home Biography Vermont Issues Press Office Services Search

Electronic Frontier Foundation Request for Expedited FOIA Processing
December 6, 2006

Exhibit 6

http://www.latimes.com/news/nationworld/nation/la-na-screening6dec06,1,7881928.story?coll=la-headlines-nation

Traveler risk assessment system gets more review

From the Associated Press

December 6, 2006

WASHINGTON — Under pressure from Congress and the public, the Homeland Security Department has extended the time for people to comment on its computerized risk assessment system for international travelers, a spokesman said Tuesday.

The deadline was pushed back from Monday to Dec. 29, spokesman Jarrod Agen said.

By Tuesday, the department had received 59 public comments. All but one either opposed the system outright as a violation of privacy and other laws or called for better means for people to correct any errors in the data.

Rep. Bennie Thompson (D-Miss.), who will become chairman of the House Homeland Security Committee in January, wrote Homeland Security Secretary Michael Chertoff seeking extension of the comment period.

Based on a briefing that committee staff received about the system Friday, Thompson wrote that "serious concerns have arisen that, with respect to U.S. citizens and possibly lawful permanent aliens, some elements of ATS as practiced may constitute violations of privacy or civil rights."

The Associated Press reported Thursday that for four years Customs and Border Protection agents have been using the Automatic Targeting System, or ATS, to produce assessments of the risk that any of the millions of people crossing U.S. borders, including Americans, are terrorists or criminals.

Almost every traveler entering or leaving the country is evaluated by the ATS computers, but they are not allowed to see the assessment of them or directly challenge its accuracy.

Exhibit G

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

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

Homeland Security

Privacy Office DHS-D3

December 14, 2006

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

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

Dear Mr. Sobel:

This is in further response to your Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS), dated November 7, 2006, requesting DHS records concerning the Automated Targeting System (ATS). Subsequent to acknowledging receipt of your request, we received a second request, dated December 6, 2006, seeking additional records pertaining to the ATS. As these two requests are directly related, we have aggregated them to simplify processing. The following is a consolidated list of records requested:

1. All Privacy Impact Assessments prepared for the ATS system or any predecessor system that served the same function but bore a different name.
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.
4. All System of Records Notices (SORNs) that discuss or describe targeting, screening, or assigning "risk assessments" of U.S. citizens by CBP or its predecessors.
5. All records that discuss or describe the redress that is available to individuals who believe that the ATS contains or utilizes inaccurate, incomplete or outdated information about them.
6. All records that discuss or describe the potential consequences that individuals might experience as a result of the agency's use of the ATS, including but not limited to arrest, physical searches, surveillance, denial of the opportunity to travel, and loss of employment opportunities.
7. 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.
8. All complaints received from individuals concerning actions taken by the agency as a result of ATS "risk assessments" or other information contained in the ATS, and the agency's response to those complaints.

9. All records that discuss or describe Section 514 of the Department of Homeland Security Appropriations Act, 2007, P.L. 109-295 (H.R. 5441) and its prohibition against the development or testing of "algorithms assigning risk to passengers whose names are not on Government watch lists."

10. All records that address any of the following issues:

    a. Whether a system of due process exists whereby aviation passengers determined to pose a threat are either delayed or prohibited from boarding their scheduled flights may appeal such decision and correct erroneous information contained in the ATS;

    b. Whether the underlying error rate of the government and private databases that will be used in the ATS to assign a risk level to an individual will not produce a large number of false positives that will result in a significant number of individuals being treated mistakenly or security resources being diverted;

    c. Whether the agency has stress-tested and demonstrated the efficacy and accuracy of all search tools in the ATS and has demonstrated that the ATS can make an accurate predictive assessment of those individuals who may constitute a threat;

    d. Whether the Secretary of Homeland Security has established an internal oversight board to monitor the manner in which the ATS is being developed and prepared;

    e. Whether the agency has built in sufficient operational safeguards to reduce the opportunities for abuse;

    f. Whether substantial security measures are in place to protect the ATS from unauthorized access by hackers or other intruders;

    g. Whether the agency has adopted policies establishing effective oversight of the use and operation of the system;

    h. Whether there are no specific privacy concerns with the technological architecture of the system;

    i. Whether the agency has, pursuant to the requirements of section 44903(i)(2)(A) of Title 49, United States Code, modified the ATS with respect to intrastate transportation to accommodate states with unique air transportation needs and passengers who might otherwise regularly trigger a high risk status; and

    j. Whether appropriate life-cycle estimates, expenditure and program plans exist.

We previously indicated in our November 14, 2006 letter, as it pertains to **Item 1**, all Privacy Impact Assessments are made available to the public via the DHS website at www.dhs.gov/xinfoshare/publications. 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 - 10** are also under the purview of CBP. Therefore, I am referring your request to the Acting FOIA Officer for CBP, Rebecca Hollaway, (Mint Annex-5th 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.

Please be advised that our office is making the determinations on any fee or treatment requests. Pertaining to your request for a fee waiver, I have reviewed your November 7, 2006 letter thoroughly and your arguments that EFF is entitled to a blanket waiver of all fees associated with this FOIA request. I have determined that you have not presented a convincing argument that EFF is entitled to a waiver of fees. Other than broad generalizations, you have not demonstrated with the requisite specificity that public interest on this issue exceeds a general level of interest in the operations and activities of a

government entity or how disclosure will enlighten the public on privacy protections and contribute to an understanding of government operations or activities. Additionally, you have not sufficiently revealed how the requested information will be widely distributed, other than the nebulous, "EFF will make the information it obtains under the FOIA available to the public and the media through its website and newsletter…" nor have you presented evidence of a unique capability to educate the public beyond EFF's constituency and similar groups which have the same concerns. For these reasons, I have determined that to furnish the information to EFF at no cost does not outweigh the burden that will be placed on our components in supplying the records. Therefore, I am denying the request for a waiver of fees.

Provisions of the Act allow us to recover part of the cost of complying with your request. We shall charge you for records in accordance with the DHS Interim FOIA regulations as they apply to media requestors. As a media requestor you will be charged 10-cents a page for duplication, although the first 100 pages are free. As the duplication fees are likely to exceed the $25.00 minimum, we need a fee payment commitment by December 29th. We initially indicated that each DHS component would make independent determinations on your various treatment requests. Please be advised that our office is making the overall determinations on these issues.

As it relates to your request for expedited treatment, your request is denied. Pursuant to 5 U.S.C. §§552 (a)(6)(E)(i), each agency shall promulgate regulations providing for expedited processing of records. Accordingly, §5.5(d) of the DHS Interim FOIA and Privacy Act regulations, 6 C.F.R. Part 5, addresses the Department's criteria for granting expedited treatment. You do not qualify for either category. Clearly, the lack of expedited treatment in this case will not pose an imminent threat to the life or physical safety of an individual. In addition, you are not primarily engaged in the disseminating of information to the public, nor have you detailed with specificity why you feel there is an urgency to inform the public about this topic. This urgency would need to exceed the public's right to know about government activity generally. Finally, you did not offer any supporting evidence of public interest that is any greater than the public's general interest in personal privacy protection.

You have the right to appeal the determination to deny you a fee waiver or expedited treatment. Should you wish to do so, you must send your appeal within 60 days of receipt of this letter by writing to the following address: Office of the General Counsel, Department of Homeland Security, Washington, D.C. 20528. Your envelope and letter should be marked "Freedom of Information Act Appeal." The implementing Department Regulations establish the criteria under which the FOIA is administered. Copies of the FOIA and Regulations are available at www.dhs.gov.

If you have any questions regarding this matter, please refer to **DHS/OS/PRIV 07-160/Sobel request**. The DHS Privacy Office can be reached at 571-227-3813. Please refer to the above mentioned identifier in any future correspondence.

Sincerely,

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

Cc: Rebecca Hollaway, CBP

Exhibit H

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

(b2)

From: (b6)
Sent: Monday, December 04, 2006 2:10 PM
To: (b6)
Cc: (b6)
Subject: ATS Talking Points and Background
Attachments: Privact Impact Assessment TPs (11.21.2006).doc; ATS-P TPs.doc

(b6)

Last Friday several media outlets were reporting on CBP's Automated Targeting System (ATS) System of Records Notice (SORN) that was published in the Federal Register. ATS is an Intranet-based enforcement and decision support tool that is the cornerstone for a CBP's targeting efforts. In an effort to prepare you for any questions you might receive on the program, please find attached the DHS Talking Points on the issue and a background paper by CBP on the issue. The Talking Points have been cleared, but the "Fact and Assertion" piece of the CBP paper has yet to receive formal DHS clearance.

(b6)

(b6)
Policy Advisor
Transportation and Infrastructure Security Policy
Office of Policy Development
Department of Homeland Security
(b2&b6)

(b2)

Automated Targeting System Talking Points

- To provide expanded notice and transparency to the public, the Department of Homeland Security, U.S. Customs and Border Protection gave notice regarding the Automated Targeting System (ATS) on November 2, 2006 in the Federal Register. This Privacy Impact Assessment provides additional details about the privacy impact associated with this system.
- ATS is not a new program nor does it represent a new collection of information. ATS was initially deployed in the early 1990's to identify cargo that was likely to be entering the United States in violation of U.S. law. Passenger modules were first deployed in the mid 1990's.
    - This assessment is being published now to provide the public with greater visibility into an existing program.
    - ATS is the enforcement screening module associated with the Treasury Enforcement Communications System and was previously covered by the Treasury Enforcement Communications System "System of Records Notice."
- ATS is the primary tool used by CBP to prescreen cargo and travelers destined to the United States. In many cases, it is the United States government's first opportunity to determine whether a good or person presents a risk of terrorism, illegal immigration, trafficking or other criminal activities. Without ATS the United States would be blind to potential threats until they have entered the United States and screening at points of entry would be slower and more cumbersome.
    - ATS treats all passengers and cargo equally. It does not profile on race, ethnicity or arbitrary assumptions.
    - ATS makes an assessment in advance of arrival based on information that DHS would otherwise collected at the point of entry.
    - ATS does not replace human decision making. It provides analysis for use by trained law enforcement officials.
- Significant system safeguards have been put in place to protect the traveling public from the unauthorized disclosure of their personal information. Access to ATS is only given to personnel with a need to access information in the course of completing their official duties and stiff penalties are associated with misuse. Auditing systems have been established to identify unauthorized access and misuse.
- Individuals may seek access to the source information collected in ATS or originating from a government source system pursuant to the FOIA and as a matter of CBP policy.

- 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 CBP is engaging in additional scrutiny, nor should he or she as this may compromise the means and methods of how CBP came to require further scrutiny.

- ATS stores data for 40 years because a recently identified transnational criminal or terrorists travel history is frequently relevant to assessing the risk they present and, when appropriate, developing a case against them. To prematurely delete data already collected under existing statutory authority would severely hamper these efforts with minimal impact on an individual's privacy.
    - This retention period for data in ATS reflects the longest underlying retention period for the data in its source records (for example, data from ACS, AMS, and ACE is retained for six years).
    - However, the touchstone for data retention, however, is its 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.

Background on ATS System

- The Automated Targeting System (ATS) is an Intranet-based enforcement and decision support tool that is the cornerstone for all Customs and Border Protection's (CBP) targeting efforts.
    - CBP uses ATS 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.
    - In this way, ATS allows CBP officers to more effectively and efficiently focus their efforts on cargo shipments and travelers that most warrant further attention.
    - ATS standardizes names, addresses, conveyance names, and similar data so these data elements can be more easily associated with other business data or 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 shipment processed through ATS is subjected to a real-time rule based evaluation.

- 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. (in development)
- ATS- -Trend Analysis and Analytical Selectivity Program, (ATS-TAP) (analytical module)

- Generally, ATS collects and maintains personal 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.
  - ATS does not collect information directly from individuals. The information used by ATS to build the risk assessment is collected from government data sources and from entities providing data in accordance with U.S. legal requirements or other applicable arrangements (e.g., air carriers providing PNR regarding individual passengers).
  - Relevant data, including personally identifiable information, is necessary for CBP to effectively and efficiently assess 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.

Exhibit I

Electronic Frontier Foundation v. Dep't of Homeland Security
Civil Actions Nos. 06-1988 & 06-2154

Plaintiff's Motion for Partial Summary Judgment

Statement
United States Senate Committee on the Judiciary
Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs
January 10, 2007

The Honorable Patrick Leahy
United States Senator , Vermont

Opening Statement of Senator Patrick Leahy

Senate Judiciary Committee

Hearing on "Balancing Privacy and Security:

The Privacy Implications of Government Data Mining Programs"

January 10, 2007

Today, the Senate Judiciary Committee holds an important hearing on the privacy implications of government data mining programs.

This Committee has a special stewardship role in protecting our most cherished rights and liberties as Americans, including the right to privacy. Today's hearing on government data mining programs is our first in the new Congress. It is the first of what I plan to be a series of hearings on privacy-related issues throughout this Congress.

The Bush Administration has dramatically increased its use of data mining technology -- namely, the collection and monitoring of large volumes of sensitive personal data to identify patterns or relationships. Indeed, in recent years, the federal government's use of data mining technology has exploded, without congressional oversight or comprehensive privacy safeguards. According to a May 2004 report by the General Accounting Office, at least 52 different federal agencies are currently using data mining technology, and there are at least 199 different government data mining programs operating or planned throughout the federal government.

Advances in technologies make data banks and data mining more powerful and more useful than ever before. These can be valuable tools in our national security arsenal, but we need to ensure we use them appropriately and with the proper safeguards so that they can be most effective.

One of the most common – and controversial – uses of this technology is to predict who among our 300 million people are likely to be involved in terrorist activities. According to the GAO and a recent study by the CATO Institute, there are at least 14 different government data mining programs within the Departments of Defense, Justice, Homeland Security and Health. That does not include the NSA's programs.

Congress is overdue in taking stock of the proliferation of these databases that increasingly are collecting

and sifting more and more information about each and every American.

Although billed as counterterrorism tools, the overwhelming majority of these data mining programs use, collect, and analyze personal information about ordinary American citizens. Despite their prevalence, these government data mining programs often lack adequate safeguards to protect privacy and civil liberties.

Just recently, we learned through the media that the Bush Administration has used data mining technology secretly to compile files on the travel habits of millions of law-abiding Americans. Incredibly, under the Department of Homeland Security's Automated Targeting System program ("ATS"), our government has been collecting and sharing this sensitive personal information with foreign governments and even private employers, while refusing to allow U.S. citizens to see or challenge their own so-called "terror scores."

Following years of denial, the Transportation Security Administration ("TSA") has finally admitted that its controversial "Secure Flight" data mining program – which collects and analyzes airline passenger data obtained from commercial data brokers – violated federal privacy laws by failing to give notice to U.S. air travelers that their personal data was being collected for government use.

And last month, The Washington Post reported that the Department of Justice will expand its ONE-DOJ program – a massive data base that will allow state and local law enforcement officials to review and search millions of sensitive criminal files belonging to the FBI, DEA and other federal law enforcement agencies. This will make sensitive investigative information about thousands of individuals – including those who have never been charged with a crime – available to local and state law agencies.

Without the proper safeguards and oversight of these and other government data mining programs, the American people have neither the assurance that these massive data banks will make us safer, nor the confidence that their privacy rights will be protected. In addition, there are legitimate questions about whether data mining technology is actually effective in identifying risks or terrorists.

A recent CATO Institute study also found that data mining is not an effective tool for predicting or combating terrorism, in part because of the high risk of false positive results. A front-page article several months ago included interviews with experts who conceded how ineffective and haphazard these programs have been. We need look no further than the government's own terrorist watch list, which now contains the names of more than 300,000 individuals – including infants, nuns, and even members of Congress – to understand the inefficiencies that can result from data mining and government dragnets. If these databases are being used in ways that create more wheel-spinning that saps critical investigative resources from effective tasks, we need to know that so we can use our tools and our talent more efficiently to get the real results in needed in thwarting terrorism. We also need to understand that a mistake in a government data base could cost a person his or her job, sacrifice their liberty, and wreak havoc on their life and reputation.

Given the many challenges posed by this technology, we in Congress must do our part to examine data mining technology and to ensure that government data mining programs actually do keep Americans safe – not just from enemies abroad, but also from abuses at home.

We begin that important task today. I am joining with Senator Feingold, Senator Sununu and others in a

bipartisan attempt to provide congressional oversight to these programs. We are introducing the Federal Agency Data Mining Reporting Act of 2007. This threshold privacy legislation would begin to restore key checks and balances by requiring federal agencies to report to Congress on their data-mining programs and activities. We joined together to introduce a similar bill last Congress. Regrettably, it received no attention. This year, I intend to make sure that we do a better job in considering Americans' privacy, checks and balances, and the proper balance to protect Americans' privacy rights while fighting smarter and more effectively against security threats.

This legislation takes a crucial first step in addressing these concerns by pulling back the curtain on how this Administration is using this technology. It does not prohibit the use of this technology, but rather provides an oversight mechanism to begin to ensure it is being used appropriately and effectively. Our bill would require federal agencies to report to Congress about its data mining programs. The legislation provides a much-needed check on federal agencies to disclose the steps that they are taking to protect the privacy and due process rights of American citizens when they use these programs.

We need checks and balances to keep government data bases from being misused against the American people. That is what the Constitution and our laws should provide. We in Congress must make sure that when our government uses technology to detect and deter illegal activity, the government does so in ways that also protect our most basic rights and liberties, and in ways that limit opportunities for abuse of these powerful tools. Our bill advances this important goal.

I thank Chairman Specter for scheduling this hearing at my request while the Republican caucus proceeds to deliberate Committee reorganization, and I thank our distinguished panel of witnesses for appearing here today.

THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

O R D E R

UPON CONSIDERATION of plaintiff's motion for partial summary judgment on the issue of its entitlement to expedited processing of requests submitted to defendant Department of Homeland Security under the Freedom of Information Act, 5 U.S.C. § 552, defendant's opposition, and the entire record, it is this ____ day of _____, 2007;

ORDERED that plaintiff'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 expedited production of responsive documents.

_____
UNITED STATES DISTRICT JUDGE