The Identity Project

www.PapersPlease.org

Edward Hasbrouck v. U.S. Customs and Border Protection

Privacy Act and FOIA (Freedom of Information Act) lawsuit for records of DHS surveillance of travelers

filed August 25, 2010, in San Francisco
(case C 10-03793 RS, U.S. District Court, Northern District of California)
initial case management conference scheduled for Thursday, January 6, 2011

See <http://www.papersplease.org/wp/hasbrouck-v-cbp/> for more information.

What is this case about? "This complaint concerns the failure to disclose records regarding the warrantless, suspicionless dragnet collection and maintenance of Federal government records of the travel, activities, and other personal information concerning U.S. citizens not accused of any crime."

Why are you suing the Department of Homeland Security? The facts leading up to the filing of this lawsuit are summarized in the initial complaint:

> In November, 2006, Defendant CBP, an agency within the Department of Homeland Security, revealed that it was already operating a system of records — for which, despite the requirements of the Privacy Act, no prior System of Records Notice ("SORN") had been promulgated — which it labeled the "Automated Targeting System" ("ATS"). According to the SORN, ATS contained records related to international travel by U.S. citizens and others, including complete airline reservations or "Passenger Name Records" (PNRs), used among other purposes for making "risk assessments" of travelers. In 2007, in his capacity as a member of the news media and a consultant to the Identity Project ("IDP) on travel-related technical, civil liberties, and human rights issues, Plaintiff Edward Hasbrouck requested copies of his own records pursuant to his right of access under the Privacy Act.
>
> When he received a response which appeared manifestly incomplete and which invoked FOIA exemptions clearly inapplicable to records required to be released pursuant to the Privacy Act, Hasbrouck appealed. Almost three years later, he has received no acknowledgment or response to that appeal.
>
> In October 2009, Hasbrouck tried again, filing a new, broader Privacy Act request to CBP for his own travel-related records from ATS and other CBP systems of records and an accounting of when and to whom they had been disclosed by CBP, a FOIA and Privacy Act request for records concerning what had happened to his 2007 request and appeal, and a FOIA request for general information concerning the indexing, search, and retrieval capabilities of the ATS records system. When

Hasbrouck received no response, he appealed the constructive denial of each of these requests. Nine months after making these requests and seven months after making these appeals, he has received no information in response.

Who is Edward Hasbrouck?

The plaintiff, Edward Hasbrouck, is an award-winning travel journalist, author, blogger, and consumer advocate. As an expert in airline reservation systems, he has testified before the TSA, the DHS Data Privacy and Integrity Advisory Committee, the European Parliament, the Canadian House of Commons, and other government agencies.

What is "U.S. Customs and Border Protection"?

The defendant, U.S. Customs and Border Protection (CBP), is an agency within the Department of Homeland Security. CBP operates the "Automated Targeting System" (ATS), a comprehensive travel surveillance and control system integrated with international airline and other travel reservation systems.

What is the "Automated Targeting System" (ATS)?

The "Automated Targeting System" (ATS) is an illegal and initially secret system of records about everyone — including U.S. citizens, regardless of whether they are suspected of any crime — who travels internationally to, from, or via the U.S. CBP (and its predecessor, the U.S. Customs Service) have been operating this system under various names since at least the mid to late 1990s.

From the start, this system of records was entirely illegal. Until 2006, its operation was a criminal violation of the Privacy Act on the part of the responsible agency employees because no proper notice of its existence had been published in the Federal Register. The inclusion of records of activities protected by the First Amendment — such as acts of assembly — also violated and continues to violate the Privacy Act. The use of this system to restrict freedom of movement, without due process or judicial review, violates U.S. international human rights treaty obligations under Article 12 (Freedom of Movement) of the International Covenant on Civil and Political Rights. (Our formal complaints of these violations, filed with the DHS, have been ignored, and the DHS has falsely claimed in official reports to European Union officials that it has received no such complaints.) And the assignment of ATS risk scores to travelers who weren't on specific watch lists violated an express Congressional prohibition.

CBP disclosed the existence of ATS in a "System of Records Notice" (SORN) in the Federal Register in November 2006. Since then, we've been trying to find out what's in our ATS files and how they are used, get the illegally-created records expunged, get the entire illegal system shut down, and get those government officials responsible for creating and maintaining it prosecuted for their crimes.

What's in the ATS records that CBP keeps about our travels?

We don't know exactly what's in the CBP's files about us, and CBP has refused to tell us, even when we asked (as is our right under the Privacy Act). That's why we brought this lawsuit.

CBP says that ATS records include complete airline reservations or Passenger Name Records (PNRs) for all international flights to, from, or via the U.S.; other information from third parties, such as remarks about us that airlines and other travel companies enter in our reservations; and government "risk assessments" of our likelihood to commit future crimes, even if we aren't yet suspected or accused. All this information is used to determine whether or not to give airlines permission to let us board flights, and whether to subject us to more intrusive "secondary" searches or interrogation.

In our initial report on CBP's incomplete and censored responses to the first requests for ATS files, we found that they included everything from IP addresses and friends' phone numbers, to whether two people traveling together had asked for one bed or two in their hotel room, to the title of a book a traveler had with him when he passed through a CBP checkpoint. Answers to questions that seemed to be part of casual conversations with border guards about where people have been, why, and with whom turn out to have been recorded in permanent files about travelers — even if nothing illegal or suspicious was found — just in case they might later come under suspicion.

Since then, we have continued to assist travelers (including several journalists) to request their travel records and to interpret the responses. But many people who requested their travel records have received no response at all. All the responses we have seen, including CBP's response to Mr. Hasbrouck's 2007 request, have been obviously incomplete, have omitted categories of ATS records described in the official notice of the system of records, and have invoked FOIA exemptions that clearly don't apply to responses to Privacy Act requests. (The CBP's entire response to Mr. Hasbrouck's 2007 request is included in the complaint in Hasbrouck v. CBP.) Administrative appeals of these responses and non-responses have either been ignored entirely, as in Mr. Hasbrouck's case, or processed only under the more limited provisions of FOIA, even when the requests and appeals were made by U.S. citizens under the Privacy Act. So far as we can tell, despite the requirements of the Privacy Act, nobody has received CBP's complete file of travel records about them, any of their "risk assessments", or any accounting of disclosures of those records to other government agencies or third parties in the U.S. or abroad.

Is this just for international travel? What if I only travel within the U.S.?

Another division of the DHS, the Transportation Security Administration (TSA), operates a different travel-permission system for domestic U.S. flights called "Secure Flight". See our FAQ About Secure Flight for more about this scheme. The DHS says that by the end of 2011 the TSA's Secure Flight system will be used for all travel permission decisions,

even for international flights. But we don't know how ATS data is being used, or will be used, by the TSA in Secure Flight decision-making.

One of the things to which we are entitled under the Privacy Act, which we have asked for, and which the CBP has failed to provide, is an "accounting of disclosures" which would indicate — among other things — whether our ATS data has been passed on by the CBP to the TSA. So far as we can tell from the responses to other people's requests that we have reviewed, the CBP has consistently and completely ignored all requests for an accounting of disclosures of ATS records.

How are these travel records used to decide whether to allow us to travel?

We don't know. The algorithms are secret, and both the ATS and Secure Flight travel surveillance and permission systems remain secret black boxes.

Why is this case important?

Since September 11, 2001, government surveillance has focused on travel, particularly air travel. The Department of Homeland Security has taken a leading role in surveillance, and acquired massive archives of personal data about innocent people. After the IRS and Social Security databases, the ATS is probably the third-largest U.S. government database of personal information about civilians who have not been accused of any crime. DHS has a secret file about you, compiled primarily from airlines and other unverified commercial sources but also containing a secret "risk assessement" they have assigned to you. DHS "shares" this information with other agencies and foreign governments, and uses this information to decide what to "allow" you to do, and where to "allow" you to go in the exercise of your right to travel.

Today, efforts to challenge the secrecy of this travel surveillance and control system have the same significance that the first cases brought against the FBI after the enactment of the Privacy Act and FOIA, challenging the secrecy of FBI files and Cointelpro programs directed at innocent Americans and foreigners alike, had in the 1970s.

So far as we know, this is the first lawsuit brought under the Privacy Act challenging CBP's failure to disclose ATS records about air travelers, to disclose how CBP handles requests for ATS records and appeals of those requests, or to disclose how ATS records are indexed and retrieved to find "links" between travelers (i.e guilt by association).

This case is also important because it puts the lie to DHS's claims to have complied with all requests for PNR data, and to have received no complaints concerning its use. These repeated, deliberate, public falsehoods have been made by U.S. officials with the intent to deceive the traveling public and foreign governments, including the European Union, who are actively debating whether to collaborate with, or even to emulate within their own countries, U.S. schemes for dragnet surveillance and permission-based control of travelers:

- In December 2008, the DHS's Chief Privacy Officer said in a report directed to the EU (page 4 of the PDF) that, "The Privacy Office received no reports of misuse of PNR since … 2005″, despite our specific formal complaints of misuse of PNR data in the ATS, in violation of U.S. law including the Privacy Act, which were filed with the DHS Privacy Office in their regulatory docket on the ATS during that time.

- In April, 2010, a review team from the E.U. reported (page 29 of the PDF), following meetings and the exchange of diplomatic notes with DHS, that, "During 2009 CBP received approximately 25,000 requests for access to data. 50% of such requests were related to traveler data…. DHS confirmed that all requests for access have been successful and passengers were always given access to their data." That was a lie: Even as a U.S. citizen, Mr. Hasbrouck received no response whatsoever to his 2009 Privacy Act request for his PNR and other travel data from CBP. That's why he filed this lawsuit.

This case presents a rare opportunity to obtain a public accounting of disclosures of travel surveillance records by CBP to other agencies, governments in the U.S. and abroad, and third parties. In February, 2010, CBP promulgated new rules that purport to exempt ATS travel records from the requirement of the Privacy Act to provide, on request, an accounting of what information has been disclosed, when, and to whom. These regulations are contrary to U.S. law and to U.S. commitments to the E.U. But unless these rules are overturned, only by diligently pursuing — and if necessary, as in this case, litigating — requests such as Mr. Hasbrouck's that were made before the rules were changed will we be able to find out with whom CBP has "shared" its dossiers about our travels.

The requested records of what happened to Mr. Hasbrouck's first Privacy Act request and appeal, which disappeared into a black hole as soon as CBP signed the receipt for the appeal letter in 2007, and hasn't been acted on or heard from since despite numerous follow-up inquiries, may also help reveal whether such requests for PNR and ATS data were among those that were improperly delayed or blocked by high-level political officials within the executive branch of the U.S. government.

Finally, this case is important because foreigners have no rights under the U.S. Privacy Act, despite being subjected to U.S. government surveillance of their travels. Only a U.S. citizen or resident, such as Mr. Hasbrouck, has standing to challenge these violations of the rights of every traveler to, from, or via, the U.S., regardless of their citizenship or place of residence.

There has been one previous lawsuit against CBP for failing to disclose ATS travel records, brought by the Electronic Frontier Foundation on behalf of a Member of the European Parliament who had traveled to the U.S. on official business. Mr. Hasbrouck participated in that case as an expert witness. In that case, as in this one, the plaintiff

received no information from CBP until she sued. But because the plaintiff in that case was not a U.S. citizen or resident, she was able to bring her case only under the much more limited rights of FOIA, and not under the Privacy Act. Much more information is exempt from disclosure under FOIA than under the Privacy Act, and FOIA does not provide for any accounting of disclosures. Although that lawsuit was, within the limits of FOIA, "successful", the plaintiff received only partial, redacted copies of her PNR data after she sued, and no accounting of disclosures of her data by CBP.

By bringing this lawsuit, we are seeking to expose the workings of DHS systems for travel surveillance and control, and vindicate the human rights and freedom to travel of visitors to the U.S. from around the world, to whom the doors to U.S. courts have been unfairly barred.

What are you asking the court to do?

The complaint in Hasbrouck v. CBP asks the court to issue a formal "Declaratory Judgment" that CBP has violated the Privacy Act and FOIA, and a court order for CBP to comply with the law, search for, and disclose all of the records about Mr. Hasbrouck's travel and the ATS records system he has requested and to which he is entitled by law, including an accounting of CBP disclosures of those records to other government agencies or third parties.

Are you afraid that the government will retaliate against you for filing this lawsuit by putting you on the no-fly list or harassing you whenever you travel?

Yes, we are. Mr. Hasbrouck is especially concerned because, as an international travel writer, his livelihood depends on his ability to travel. But somebody had to do this. If nobody stands up to scary government bullies, their bullying will continue indefinitely. Any retaliatory harassment of us, or interference with our travels, would itself be a serious violation of our civil, Constitutional, and human rights, including our right to travel.

What is the Identity Project? The Identity Project (http://www.PapersPlease.org) provides advice, assistance, publicity, and legal support to those who find their rights infringed, or their legitimate activities curtailed, by demands for ID, and builds public awareness about the effects of ID requirements on fundamental rights. We are part of the First Amendment Project, a 501(c)(3) nonprofit organization based in Oakland, CA.

What can I do to help?

Contribute to the Identity Project to carry on this work. Request your own travel records from CBP. Spread the word. Tell your friends. Post a link to this page in your blog. Stand up for your own rights, and "just say no" to demands for ID, permission to travel, or warrantless, suspicionless surveillance of travelers. See our website or contact us for more on how to get involved.