I. Issue: Surveillance and Monitoring of Travelers

II. Reporting Organizations: The Identity Project (PapersPlease.org)[1] and the Consumer Travel Alliance (ConsumerTravelAlliance.org)

The Identity Project (IDP), <http://www.PapersPlease.org>, provides advice, assistance, publicity, and legal defense to those who find their rights infringed by demands for identification. IDP is a program of the First Amendment Project, a nonprofit organization dedicated to protecting rights protected by the First Amendment to the U.S. Constitution and international human rights treaties.

The Consumer Travel Alliance (CTA), <http://www.consumertravelalliance.org>, is a nonprofit, nonpartisan organization that works to provide consumers an articulate and reasoned voice in decisions that affect travel consumers. CTA is one of the member organizations of the Consumer Federation of America.

III. Issue Summary

Since the U.S. Second and Third Periodic Reports to the UNHRC, the U.S government has implemented an increasingly comprehensive system of surveillance of travel and movement, compiling a detailed, secret, lifetime "travel history" for each international traveler and many domestic travelers, including those who are not suspected of any crime and not the subject of any investigation.

Pursuant to the Secure Flight[2] (domestic air travel), APIS[3] (international air and surface travel including trains, buses, and ships), and PNR (international air travel) regulations, each passenger is required to provide uniquely identifying information to the common carrier, and the carrier is required to transmit this identifying information and detailed itinerary and other information about the passenger to the U.S. Department of Homeland Security (DHS).

Under U.S. law, personal information provided to a third party, such as an airline, is considered the exclusive and unencumbered property of that third party, even when that information is provided as a condition of the exercise of a right. The third party may then "voluntarily" provide this information to the government, without notice or consent of the data subject, without implicating the Fourth Amendment to the U.S. Constitution or requiring any warrant or court order.

The DHS Automated Targeting System (ATS, system of records DHS/CBP-006) and related

---

1 Contact for this submission: Edward Hasbrouck, <eh@papersplease.org>, telephone +1-415-824-0214

2 Comments of the Identity Project, "Secure Flight Program" (October 22, 2007), <http://hasbrouck.org/IDP/IDP-SecureFlight-comments.pdf>; "Secure Flight FAQ", <http://papersplease.org/sf_faq.html>.

3 Comments of the Identity Project, "Passenger Manifests for Commercial Aircraft Arriving in and Departing From the United States" (October 12, 2006), <http://hasbrouck.org/IDP/IDP-APIS-comments.pdf>.

DHS systems of travel records[4] include complete copies of all international airline reservations ("Passenger Name Records", PNRs); logs of all entries, exits, and border crossings by any means of transport (including vehicle license plate numbers obtained from automated readers that scan all vehicles in the vicinity of border crossings); and unfiltered free-text notes and remarks by customs and immigration inspectors and airline and travel agency personnel.[5]

PNRs can include such sensitive information as whether a traveler requested a halal or a kosher meal, details of invisible medical conditions, or whether two travelers asked for one bed or two in their shared hotel room.[6] PNRs include cellphone and credit card numbers, IP addresses, and other personal identifiers. ATS also is linked to, and accesses, records of "commercial data aggregators".[7]

"Routine uses" of ATS records include disclosure to other government agencies in the U.S. and other countries. No logs are kept of who retrieves ATS records. Travelers are required by law to provide information to airlines, but airlines are allowed to use that information without notice to or consent of travelers.

For domestic airline travel within the U.S., Secure Flight passenger data including unique passenger identifiers and complete flight itinerary details can be retained by the DHS for 99 years if the traveler is on any "watch" list. Any government agency can place anyone on a watch list if the agency wants to trigger retention of records of that person's travel. There are no published standards for watch lists.

ATS and Secure Flight records are used, in accordance with secret algorithms, as part of the basis for "fly/no-fly" decisions, profiling of travelers, assignment of "risk assessment" scores, and selection of certain travelers for "secondary" (more intrusive) screening, search, and/or interrogation. ATS and Secure Flight records are also used for "social network analysis" of associations between travelers, as part of a suspicion-generating system of guilt by association.

Rather than treating travel as a protected activity (as claimed in Paragraph 251 of the U.S. Fourth Periodic Report), the U.S. treats travel – whether on public rights-of-way or by common carrier – as an inherently suspicious activity that justifies warrantless, suspicionless dragnet surveillance and logging. Surveillance of travelers has been subjected to reduced, not heightened, scrutiny by U.S. courts.[8]

---

4 Additional DHS systems of travel records linked to ATS include the Advance Passenger Information System (APIS, DHS/CBP-005), Border Crossing Information System (BCIS, DHS/CBP-007), U.S. Customs and Border Protection TECS (DHS/CBP–011), Non-Federal Entity Data System (NEDS, DHS/CBP-008), DHS Use of the Terrorist Screening Database (TSDB) System of Records (DHS /ALL-030), Electronic System for Travel Authorization (ESTA, DHS/CBP-009), and Nonimmigrant Information System (NIIS, DHS/CBP-016).

5 See examples of these records at <http://hasbrouck.org/articles/Hasbrouck-BrennanCenter-3OCT2012.pdf>.

6 See Edward Hasbrouck, "What's in a PNR?", <http://hasbrouck.org/articles/PNR.html>.

7 ATS, System of Records Notice (SORN), 77 Federal Register 30297-30304 (May 22, 2012)

8 See complaints of the Identity Project that the ATS, Secure Flight, and other travel surveillance and control systems violate Article 12 of the ICCPR, filed in DHS rulemakings from 2006 to 2009 and resubmitted to the designated DHS point of contact for complaints of human rights treaty violations on August 10, 2010,

Knowing that all of one's travels will be logged by the government, and that one may be questioned, years later, about the details of one's travels or associations with other travelers, exerts a chilling effect on the exercise of rights to travel, assembly, and association. Many people chose not to travel to or via the U.S. to avoid this surveillance. U.S. citizens and residents, however, cannot escape it, especially if they live in any of the U.S. island territories accessible only by air.

IV. U.S. Government Report

The U.S. Fourth Periodic Report does not mention any of the U.S. government's programs for collection of information about travelers and their movements, despite complaints that they violate U.S. obligations pursuant to the ICCPR.

Paragraph 251 of the U.S. Fourth Periodic Report claims that, "governmental actions affecting travel are subject to … heightened judicial review", but does not mention the exemption of DHS systems of travel records from the provisions of the Privacy Act for judicial review of accuracy, relevance, and necessity.

Paragraphs 321-335 of the U.S. Fourth Periodic Report discuss the rules for searches pursuant to the Fourth Amendment to the U.S. Constitution, but do not mention the "third party" exception to the Fourth Amendment for information obtained by the government from commercial or other intermediaries.

Paragraph 328 of the U.S. Fourth Periodic Report discusses the Privacy Act, including its requirements for relevance and necessity of government records, but does not mention that the DHS has exempted its systems of travel records from those provisions of the Privacy Act as well as the provisions for access to records by data subjects, accounting of disclosures to third parties, and correction of records. These exemptions have been upheld by all U.S. courts that have reviewed them.[9] Only "U.S. persons" (citizens and residents) have any rights under the Privacy Act. Foreign visitors have no rights under the Privacy Act.

V. Legal Framework

ICCPR Article 12: "Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence.... Everyone shall be free to leave any country, including his own.....
No one shall be arbitrarily deprived of the right to enter his own country."

ICCPR Article 17: "ICCPR Article 17: "No one shall be subjected to arbitrary or unlawful interference with his privacy.... or correspondence."

<http://papersplease.org/wp/wp-content/uploads/2010/08/tsa-ocrcl-10aug2010-attach.pdf>.

9 Edward Hasbrouck v. U.S. Customs and Border Protection, <http://papersplease.org/wp/hasbrouck-v-cbp/>.

ICCPR Article 21: "The right of peaceful assembly shall be recognized."

ICCPR Article 22: "Everyone shall have the right to freedom of association."

General Comment No. 27: Freedom of movement (Art. 12): "It is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them. Restrictive measures … must be appropriate to achieve their protective function; [and] they must be the least intrusive instrument amongst those which might achieve the desired result.... States should ensure that ... reasons for the application of restrictive measures are provided.... The application of restrictions in any individual case must be based on clear legal grounds and meet the test of necessity."

VI. Recommended Questions

(1) Does the U.S. believe that travel is, in itself, sufficient basis to require disclosure of personal information (either directly or through common carriers), or to authorize government access to, and retention of, commercial travel records?

(2) Does the U.S. believe that the right to privacy is limited to U.S. persons?

VII. Suggested Recommendations

(1) Neither disclosure of personal information to travel companies, nor "consent" for government access to any such information, should be required as a condition of the exercise of the right to freedom of movement, assembly, or association.

(2) Records of travel or other activities protected by the ICCPR should be maintained only on the basis of particularized suspicion of a specific individual, as determined in accordance with substantive and procedural due process and the standard of "necessity" defined in General Comment No. 27.

(3) The exemptions of travel records from the Privacy Act should be repealed. As records of the exercise of rights guaranteed by the ICCPR, travel records should be subjected to heightened, not reduced, requirements for access and review.

(4) Since the rights to privacy and freedom of movement are human rights shared by all individuals regardless of citizenship, the protections of the Privacy Act should be extended to all individuals regardless of citizenship.

(5) Records pertaining to non-suspects in the ATS, Secure Flight, and other systems of government travel records should be promptly purged.