U.S. Department of Homeland Security
U.S. Customs and Border Protection
Washington, DC 20229

U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy

June 21, 2013

U.S. law requires airlines operating flights to, from, or through the United States to provide the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), with certain passenger reservation information, called Passenger Name Record (PNR) data, primarily for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and certain other crimes that are transnational in nature. This information is collected from airline travel reservations and is transmitted to CBP prior to departure.

Collection of this information from air carriers is authorized by 49 U.S.C. § 44909(c)(3) and its implementing (interim) regulations at 19 CFR 122.49d. These statutory and regulatory authorities require each air carrier operating passenger flights in foreign air transportation to, from, or through the United States to provide CBP with electronic access to PNR data to the extent it is collected and contained in the air carrier's reservation and/or departure control systems.

Further, in order to permit transfers of PNR data to the U.S., the European Union (E.U.) has determined that U.S. laws, in conjunction with CBP policies regarding the protection of personal data, provide an adequate basis upon which to permit transfers of PNR data to the U.S. consistent with applicable E.U. law. An updated U.S.-E.U. PNR Agreement was signed in December, 2011.[1] Provision of this information is mandatory for all air carriers transporting people to, from, or through the United States.

1. What is the purpose for collecting PNR?

The primary purpose for soliciting this information is to enable CBP to make accurate, comprehensive decisions about which passengers require additional inspection at the port of entry based on law enforcement and other information. DHS/CBP uses PNR strictly:
(1). To prevent, detect, investigate, and prosecute:

a. Terrorist offenses and related crimes, including

[1] *Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, signed December 14, 2011 *(2011 PNR Agreement)*, available at http://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf

i. Conduct that--

1. involves a violent act or an act dangerous to human life, property, or infrastructure; and

2. appears to be intended to--

a. intimidate or coerce a civilian population;

b. influence the policy of a government by intimidation or coercion; or

c. affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking.

ii. Activities constituting an offense within the scope of and as defined in applicable international conventions and protocols relating to terrorism;

iii. Providing or collecting funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the acts described in subparagraphs (i) or (ii);

iv. Attempting to commit any of the acts described in subparagraphs (i), (ii), or (iii);

v. Participating as an accomplice in the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

vi. Organizing or directing others to commit any of the acts described in subparagraphs (i), (ii), or (iii);

vii. Contributing in any other way to the commission of any of the acts described in subparagraphs (i), (ii), or (iii);

viii. Threatening to commit an act described in subparagraph (i) under circumstances which indicate that the threat is credible;

b. Other crimes that are punishable by a sentence of imprisonment of three years or more and that are transnational in nature;

A crime is considered as transnational in nature in particular if:

i. It is committed in more than one country;

ii. It is committed in one country but a substantial part of its preparation, planning, direction or control takes place in another country;

iii. It is committed in one country but involves an organized criminal group that engages in criminal activities in more than one country;

iv. It is committed in one country but has substantial effects in another country; or

v. It is committed in one country and the offender is in or intends to travel to another country;

(2) on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court;

(3) to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination.

(4) for domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR.

2. Who is affected by the program?

All persons traveling on flights to, from, or through the United States will be affected by this program.

3. What information is collected?

The Automated Targeting System-Passenger (ATS-P), a component of ATS, maintains the PNR information obtained from commercial air carriers and uses that information to assess whether there is a risk associated with any travelers seeking to enter, exit, or transit through the United States. PNR may include some combination of the following categories of information, when available:

1. PNR record locator code.
2. Date of reservation/issue of ticket.
3. Date(s) of intended travel.
4. Name(s).
5. Available frequent flier and benefit information (i.e., free tickets, upgrades, etc.).
6. Other names on PNR, including number of travelers on PNR.
7. All available contact information (including originator of reservation).
8. All available payment/billing information (e.g. credit card number).
9. Travel itinerary for specific PNR.
10. Travel agency/travel agent.
11. Code share information (e.g., when one air carrier sells seats on another air carrier's flight).
12. Split/divided information (e.g., when one PNR contains a reference to another PNR).
13. Travel status of passenger (including confirmations and check-in status).
14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields.
15. Baggage information.
16. Seat information, including seat number.
17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information.
18. Any collected APIS information (e.g., Advance Passenger Information (API) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender).
19. All historical changes to the PNR listed in numbers 1 to 18.

Not all air carriers maintain the same sets of information in PNR, and a particular individual's PNR likely will not include information for all possible categories. In addition, PNR does not routinely include information that could directly indicate the

racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual. To the extent PNR does include terms that reveal such personal matters, DHS employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances where the life of an individual could be imperiled or seriously impaired.

4. How is the information used?

PNR data is used to assist CBP Officers in measuring the risk associated with an individual traveling to, from, or through the United States. This information helps CBP Officers determine which travelers should be subject to additional inspection or require law enforcement action.

5. Who will have access to the information?

CBP is the primary user of this information. The PNR information collected from airlines may be made available to other government agencies outside the Department of Homeland Security for law enforcement purposes pursuant to the "routine uses" included in the ATS System of Records Notice (SORN)[2] and consistent with the terms of any applicable laws, regulations, DHS policies, and international agreements/arrangements, such as the 2011 PNR Agreement. PNR information will not be shared outside of DHS unless the receiving agency has a proper need to know the information and can ensure the information will be properly protected.

6. How will the information be protected?

Personal information will be kept secure and confidential and will not be discussed with, nor disclosed to, any person within or outside CBP other than as authorized by law and in the performance of official duties, and as described above. Careful safeguards, including appropriate security controls, compliance audits, and written arrangements with non-DHS agencies will ensure that the data is not used or accessed improperly. In addition, the DHS Chief Privacy Officer will review pertinent aspects of the program to ensure that proper safeguards are in place. Roles and responsibilities of DHS employees, system owners and managers, and third parties who manage or access information in ATS-P include:

6.1 DHS Employees

As users of ATS, DHS employees:

- Access records containing personal information only when the information is needed to carry out their official duties because of a specific "need to know."

[2] DHS/CBP-006 - Automated Targeting System 77 Fed. Reg. 30297 (May 22, 2012). Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

- Disclose personal information only for legitimate official purposes and in accordance with applicable laws, regulations, and ATS routine use policies and procedures.

6.2 ATS System Owners/Managers

System Owners/Managers:

- Follow applicable laws, regulations, ATS and DHS policies and procedures in the development, implementation, and operation of information systems under their control.
- Conduct a risk assessment to identify privacy risks and determine the appropriate security controls to protect against those risks.
- Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected.
- Ensure that all processes that contain personal information have an approved Privacy Impact Assessment. Privacy Impact Assessments meet appropriate OMB and DHS guidance and will be updated as the system progresses through its development stages.
- Ensure that all personal information is protected and disposed of in accordance with applicable laws, regulations, and ATS and DHS policies and procedures.
- Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law.
- Establish and maintain appropriate administrative, technical, and physical security safeguards to protect personal information.

6.3 Third Parties

Third parties, including other law enforcement entities, who may have access to information collected by ATS shall comply with requirements of written arrangements drafted to address, among other matters, privacy issues, or shall follow the same privacy protection guidance as DHS employees.

7. What notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared?

Notice has been given to the public through the ATS SORN[3] in conjunction with the ATS PIA.[4] Because ATS does not collect PNR directly from individuals, there is no opportunity for an individual to consent to provide this information. PNR data maintained in ATS is collected from airlines in accordance with U.S. law as stated above.

---

[3] DHS/CBP-006 - Automated Targeting System 77 Fed. Reg. 30297 (May 22, 2012). Available at: http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm.

[4] Available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf

Similarly, since the PNR data is collected from the airlines to assist CBP in performing border security functions, it is not appropriate to seek consent from the affected individuals with respect to the defined uses of this information. Individuals do not have the right to consent to particular uses of the information. Once an individual submits the data to the airline for reservation purposes and the airline forwards the PNR data to CBP, the individual cannot exert control over it (except in the context of a request for access or redress, as discussed below in section 9).

8. How long is information retained?

The retention period for data maintained in ATS-P will not exceed fifteen years, after which time it will be deleted, except as noted below. The retention period for PNR, which is contained only in ATS-P, will be subject to the following further access restrictions: ATS-P users will have general access to PNR for five years, after which time the PNR data will be moved to dormant, non-operational status. After the first six months, the PNR will be "depersonalized," with names, contact information, and other personally identifiable information masked in the record. PNR data in dormant status will be retained for an additional ten years and may be accessed only with prior supervisory approval and only in response to an identifiable case, threat, or risk. Such limited access and use for older PNR strikes a reasonable balance between protecting this information and allowing CBP to continue to identify potential high-risk travelers.

Notwithstanding the foregoing, information maintained only in ATS-P that is linked to law enforcement lookout records, CBP matches to enforcement activities, investigations or cases (i.e., specific and credible threats, and flights, individuals and routes of concern, or other defined sets of circumstances), will remain accessible for the life of the law enforcement matter to support that activity and other related enforcement activities.

9. Who to contact for more information about PNR in ATS-P

Any individual, regardless of citizenship who wishes to seek access to his or her PNR held by DHS can do so under the Freedom of Information Act (FOIA). FOIA provides members of the public with access to records, subject to certain exemptions, about the operations and activities of the U.S. federal government. Individuals seeking access to PNR records may submit a FOIA request to CBP at https://foia.cbp.gov/palMain.aspx, or by mailing a request to:

CBP FOIA Headquarters Office
U.S. Customs and Border Protection
FOIA Division
90 K Street NE, 9th Floor
Washington, DC 20002
Fax Number: (202) 325-0230

The Privacy Act of 1974 (5 U.S.C. § 552a) protects the personally identifiable information (PII) the federal government keeps on United States citizens and lawful permanent residents in "Systems of Records." PII is information kept by an agency that can be used to identify an individual when retrieved by name or some other personal identifier, and must be kept in a system of records. The Privacy Act regulates how the government can disclose, share, provide access to, and maintain the personal information that it collects. Not all information collected is covered by the Privacy Act. The Act's major provisions require agencies to:

- Publish a Privacy Act Notice in the Federal Register explaining the existence, character, and uses of a new or revised System of Record;
- Keep information about citizens and lawful permanent residents accurate, relevant, timely, and complete to assure fairness in dealing with such persons; and
- Allow citizens and lawful permanent residents to, upon request, access and review their information held in a System of Record.

An overview of the Privacy Act can be viewed at the following web site: http://www.justice.gov/opcl/1974privacyact-overview.htm

DHS, as a matter of policy, administratively extends Privacy Act protections, including the ability to access and amend records, to all persons, regardless of citizenship, when dealing with mixed systems (systems housing information about both U.S. citizens and foreign nationals).[5] DHS considers ATS-P to be a mixed system and permits foreign nationals to request access and amendment under the Privacy Act. However, certain information maintained in ATS-P, such as information pertaining to the rule sets or accounting of a sharing with a law enforcement or intelligence entity in conformance with a routine use, may not be accessed, pursuant to 5 U.S.C. § 552a (j)(2) or (k)(2).

Requests for access to personally identifiable information contained in ATS-P, including PNR, may be submitted to the FOIA Headquarters Office, above. Requests for information should conform to the requirements of 6 CFR Part 5, which provides the rules for requesting access to Privacy Act records maintained by DHS. The envelope and letter should be clearly marked "Privacy Act Access Request." The request should include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. The request must be signed and either notarized or submitted under penalty of perjury.

Questions, concerns, or comments of a general or specific nature regarding CBP or its handling of PNR may be directed to the CBP INFO Center. You may contact the CBP INFO Center in any one of three ways:

Online - Through the "Questions" tab at: www.cbp.gov

[5] *See* DHS Privacy Policy Memorandum Number: 2007-1 "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons," available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

Telephone - During the hours of 8:30 a.m. to 5:00 p.m. Eastern Time:
(877) 227-5511 (toll-free call for U.S. callers)
(202) 325-8000 (international callers)
(866) 880-6582 (TDD)

Mail - U.S. Customs & Border Protection
OPA/CBP INFO Center
1300 Pennsylvania Avenue N.W., MS: 1345
Washington, DC 20229

Individuals may also seek redress through the DHS Traveler Redress Inquiry Program ("TRIP"). Persons who believe they have been improperly denied entry, refused boarding for transportation, or identified for additional inspection by CBP may submit a redress request through TRIP. TRIP is a single point of contact for persons who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs – like airports, seaports, and train stations – or crossing U.S. borders. Through TRIP, a traveler can request correction of erroneous data stored in ATS-P and other data stored in other DHS databases through one application. DHS TRIP redress requests can be made online at http://www.dhs.gov/dhs-trip or by mail at:

DHS Traveler Redress Inquiry Program (TRIP)
601 South 12th Street, TSA-901,
Arlington, VA 20598-6901

In the event that a complaint cannot be resolved by CBP or through the DHS TRIP process, the complaint may be directed, in writing, to the Chief Privacy Officer, Department of Homeland Security, Washington, DC 20528-0550; Email at privacy@hq.dhs.gov; Phone: (202) 343-1717; and Fax: (202) 343-4010. The Chief Privacy Officer shall review the situation and endeavor to resolve the complaint.