Frequently Asked Questions about PNR Data

What's a PNR? A PNR ("Passenger Name Record") is a record in a database of travel reservations that contains information about the trip. A single PNR can contain data about one person or about a group of up to 100 people travelling together. It can include personal information about the travelers and other individuals, and about services provided by airlines, railroads, hotels, tour operators, etc.

Where does the data in PNR's come from? PNR's are created by travel companies such as airlines, travel agencies, and tour operators. One PNR can contain information entered by multiple travel companies in separate entries from different places at different times.

Is all the information in a PNR originally collected from the traveller? No. PNR's can contain information entered by travel companies without the knowledge of the traveler. For example, a PNR can contain free-text remarks from customer service representatives at a ticket counter or call center, or notations from a hotel or tour company about what special services or amenities were requested.

Do travellers know what personal data is entered in PNR's? No. For example, a travel agency often includes its entire "profile" of the customer in each PNR. This can include information unrelated to this trip, such as alternate contact information, memberships in other airlines' frequent-flyer programs, or details of other credit cards.

Are travellers the only data subjects of PNR's? No. PNR's contain information about other data subjects. These include travel industry workers, people who pay for other people's tickets, contact information of family or friends or business associates, addresses for ticket delivery, reconfirmation phone numbers, etc.

Do PNR's contain sensitive data? Yes. PNR's contain special meal requests that can indicate religion, and special service requests that can indicate medical conditions and disabilities. They can include billing, contact, PNR membership, and special fare eligibility information that indicates trade union or political party membership.

Can the sensitive data be filtered out? No. Each airline or travel agency has its own business practices. For example, a negotiated discount code for participants in a trade union convention may be entered in the endorsements, ticket designator, or "IT" box on the ticket, in the form-of-payment information, or in free-text remarks or "SSI" (special service information) or "SSR" (special service requests). Because of the possible variations in types of sensitive data, languages, and entry formats, it is impossible reliably to filter out sensitive data included in PNR's.

Will a "push" system protect sensitive data? No. Sensitive data could be included in the "push" fields. In particular, if free-text remarks, SSI, or SSR fields are included in the "push", sensitive data *will* be included in the push.

Where are PNR's stored? Most PNR's are hosted by Computerized Reservation Systems

(CRS's). Most airlines don't host their own PNR's. Instead, they rent a "partition" in the database of a CRS to store their PNR's. In effect, they outsource the storage of their PNR's to a CRS. Each CRS holds copies of all the PNR's for flights on the airlines that use that CRS as their "system vendor", *and* all of the PNR's created by any of the travel agencies that subscribe to that CRS, for flights on any airline or for any other travel services. CRS's are also known as "Global Distribution Systems" (GDS's) GDS's, although the term "CRS" is used in the EC "Code of Conduct for CRS's".

Where are these CRS's located? There are four major CRS's that serve most of the world's airlines and travel agencies. Three (Sabre, Galileo, and Worldspan) are owned by companies based in the U.S. One (Amadeus) is owned by a company based in the EU. All of the CRS's have redundant servers in multiple locations ("cloud computing").

Do all European airlines and travel agencies use a European CRS? No. All of the U.S.-based CRS's have substantial market share with European airlines and travel agencies. *The majority of PNR's created by travel agencies in the EU are created in CRS's in the U.S.*

What happens if the travel agency or tour operator uses one CRS, and the airline is hosted in a different one? Separate PNR's are created in *both* CRS's.

But isn't a CRS just a conveyor belt for messages between travel agencies and airlines? No. For example, if a European travel agency uses Sabre, a PNR is created in Sabre for every reservation that travel agency makes, even if it's a reservation for an airline hosted in Amadeus (for which a PNR is also created by the airline in Amadeus).

What happens if it's a "codeshare" flight labeled with flight numbers of two or more airlines? Typically, PNR's are created in the CRS's used by each of the airlines.

So even if the flight is operated by an airline hosted in Amadeus in the EU, a codeshare airline might have a PNR for the same reservation in a CRS in the U.S.? Yes.

What happens if I make my reservations on the Internet? Most online travel agencies rely on CRS's to connect them to the airlines, just like brick-and-mortar travel agencies. That means PNR's are created in the online agency's CRS as well as the airline's CRS.

So most of the time, when I make a reservation with a travel agency in the EU, on an airline based in the EU, the travel agency or tour operator sends my data to a CRS in the U.S., where a PNR is created and stored in the U.S. by the CRS before the information even comes back to the airline in Europe? Yes.

And that happens regardless of whether the flight is to, from, or via the U.S.? Yes.

Is the transfer of PNR data to a CRS in the U.S. covered by the PNR agreement? No. The agreement only applies to transfers of PNR data from an airline to the DHS. It doesn't apply to transfers of PNR or other personal data to a CRS or other commercial entity in the U.S., or indirect transfers to the DHS by way of an intermediary like a CRS.

If the DHS obtains PNR data from a CRS in the U.S., is that covered by the PNR agreement? No.

If the FBI or another U.S. government agency obtains PNR data from a CRS in the U.S., without involving the DHS, is that covered by the PNR agreement? No.

Is anything a CRS in the U.S. does with PNR data once it obtains it from a travel agency, tour operator, or airline office in the EU covered by the PNR agreement? No.

Once PNR data is transferred to a CRS in the U.S., are there any controls in U.S. law on how it is used, or on onward transfers? No.

So the transfer of PNR data to CRS's in the U.S. completely bypasses the PNR agreement? Yes.

Who can access PNR data held by CRS's? That's totally at the discretion of the CRS. Any office of an airline, anywhere in the world, can access all PNR's for all of that airline's flights worldwide. In most cases, unless the PNR has been "claimed" by a specific travel agency, any travel agency anywhere in the world can access any PNR made directly with an airline, if they know the record locator or name and flight details.

Is access limited to the travel agency or airline office that made the reservation? In general, no. Any office of that travel agency or airline can access all its PNR's.

Are there any purpose restrictions on access to PNR data held by CRS's? No. A travel agent or airline employee does not need to specify a purpose to access a PNR.

Are there any geographic restrictions on cross-border access to PNR data held by CRS's? No. CRS infrastructure is designed to ensure that all PNR data is seamlessly available to all subscribers worldwide, in real time. No special access procedures are required to access PNR's containing data entered in other jurisdictions.

Are there any restrictions on access to sensitive data in PNR's held by CRS's? No. In general, any airline office or travel agency anywhere in the world can access the entire PNR, including any sensitive data.

Are there any U.S. laws that protect PNR data held by CRS's? No. The U.S. has no general data protection law for commercial data, and no specific data protection law applicable to CRS's or PNR's. In the U.S., commercial data such as PNR's is considered to be the exclusive informational property of the company, in which the data subject has *no* rights. Under U.S. law, CRS's can legally retain PNR data forever, use it, sell it, or transfer it to anyone or anywhere in the world, including to the U.S. government or other governments, without notice or consent of the data subject. They are not required to keep records of access or transfers. They are not required to disclose PNR data or provide an accounting of disclosures, even in response to subject access requests. As for-profit companies, they have a

fiduciary duty to their stockholders under U.S. law to monetize this data, like any of their other property, if they can find a way to do so.

Do CRS's in the U.S. share PNR data with other third parties? Yes. Several data mining, profiling, and direct marketing companies in the U.S. specialize in processing PNR data. (These companies include one of the U.S. divisions of Amadeus.)

Are there any U.S. laws that protect PNR data transferred to third parties? No.

Are there any U.S. laws that limit the retention of PNR data by CRS's or other travel companies? No. CRS's and other companies in the U.S. can keep PNR's forever. So even after the DHS has deleted its copy of the PNR, it could always get a new copy from the CRS. And if the DHS has only a partial copy of a PNR, or some sensitive data has been deleted or was filtered out before the PNR was pushed to the DHS, the DHS could always get a complete copy including all the sensitive data from the CRS.

Who has jurisdiction over CRS's in the U.S.? That's not clear. In practice, they fall through a gap in jurisdiction between the Department of Transportation and the Department of Commerce. Since neither agency has clear authority over them, CRS's are effectively exempt from government oversight in the U.S.. (The Consumer Travel Alliance in the U.S. has been trying to get the DOT and FTC to agree on which of them, if either, has jurisdiction over CRS's, but without success.) In any case, their only jurisdiction would be over fraud by CRS's. As long as they don't lie about what they do, they can do anything they want with PNR's, without violating U.S. law.

Are CRS's regulated in the U.S.? No. CRS's were completely deregulated in the U.S. in 2004. Even before 2004 when CRS's were regulated in the U.S., those regulations had no provisions related to privacy or protection of personal data. (The CRS regulations in the U.S. had provisions to protect travel agency business data from being disclosed to their competitors, but nothing to protect individuals' personal data.)

Are there any U.S. laws that restrict government access to PNR data held by CRS's? No.

What about the U.S. Privacy Act? The Privacy Act only protects data held in U.S. government databases, not government access to private or commercial databases.

Does the DHS or any other U. S. Government agency need a warrant or a court order to get access to PNR data held by a CRS in the U.S.? No. Under U.S. law, the CRS can "give" the data to anyone, including government agencies.

Is there any record that a CRS or airline has ever challenged a DHS request for PNR or other personal data? No.

If a CRS or airline did challenge a request for PNR data, would the DHS need a court order or warrant to force the CRS to disclose it? No. Under the USA-PATRIOT Act, the

DHS or FBI could issue an administrative "National Security Letter" ordering a CRS or airline to turn over PNR data, and ordering them to keep the NSL secret.

Has the DHS ever done this? Since the whole process is secret, there's no way to know.

If the DHS forced a CRS to turn over PNR's from a European airline or travel agency, would the airline or travel agency know that this had happened? Probably not. A National Security Letter can include an order to keep the NSL secret.

Would the CRS's own European staff or management know that this had happened? Probably not. For example, in 2006, when the DHS revealed the existence of its "Automated Targeting System" (ATS), the President and CEO of Travelport's EMEA Division told a reporter that "there were some talks with the DHS" on access to PNR's, but that "nothing came of it.... It would have crossed my desk if it had included any PNR's from Galileo travel agencies in Europe. But so far as I know, no Galileo PNR's were provided to the U.S. government." PNR's released in response to subject access requests later revealed that Galileo PNR's were routinely included in the ATS – apparently without Galileo's most senior European manager knowing about it.

Could the DHS get access to PNR data stored by a CRS in the EU? Yes, if that CRS has any offices in the U.S. with access to that PNR data. The DHS could order a CRS office in the U.S. to retrieve the data and turn it over to the DHS, and could order that U.S. office not to tell the head office or parent company in the EU.

Has this happened? Since the whole process would be secret, and CRS's keep no access logs, there's no way to know.

Could the same thing happen in other countries? Yes. Any national government, anywhere in the world, could order a local office of the CRS, airline, or travel agency to retrieve PNR data from a CRS, and turn it over to the government. This would be especially easy in a country where the government owns, or is affiliated with, a national airline or government-run travel agency or tour operator with a CRS subscription.

Has this happened? Yes. In one case, foreign human rights lawyers were located and deported from a country based on information obtained from their PNR by the government through a local airline office or travel agency.

Do CRS's keep records of where PNR data is collected? No. It's impossible to tell whether some of the data in a particular PNR was collected in the EU.

Do CRS's keep logs of access to PNR's? No. In response to requests from data subjects, EU airlines have said that neither the airline nor the CRS has any record of who has accessed the data in any of the PNR's for their flights, even when reservations were made directly with the airline and the PNR's were created in the EU in Amadeus.

Has there been a finding that there is adequate protection for PNR data collected in the

EU and transferred to CRS's in the U.S.? No.

What about the "adequacy finding" associated with the PNR agreement? That finding was limited to transfers of PNR data from airlines in the EU to the DHS for law enforcement purposes. It did not make any finding about transfers of PNR data to commercial entities in the U.S. such as CRS's, or transfers for commercial purposes.

What about "Safe Harbor"? The company that owns the Galileo and Worldspan CRS's recently claimed that it complies with Safe Harbor. But no government agency in the U.S. has authority to audit or investigate that claim, or has actually done so. No private individual or independent watchdog organization has access to Travelport's records to audit their Safer Harbor compliance claim. However, that claim is suspect. For example, since neither Galileo nor Worldspan keeps logs of access to PNR's it would be impossible for them to comply with a subject access request for an accounting of disclosures.

Do airlines, travel agencies, and tour operators in the EU who subscribe to CRS's based in the U.S. tell their customers that they store PNR's in the U.S., even for trips within the EU or to other destinations, or obtain their consent to do so? No.

Is there any legal recourse available to a data subject whose PNR data are transferred from the EU to a CRS in the U.S. without their consent? In theory, they can complain to their national data protection authorities, or bring a lawsuit. Of course, most of the time they don't know about the transfers, so they don't know to complain.

What happens when travellers complain to national data protection authorities about transfers of their PNR data to CRS's in the U.S., or possible access from other countries? Data protection authorities lack adequate technical expertise to evaluate PNR data and claims about PNR data flows and transfers. In the absence of access logs in PNR's, it's impossible to know who has accessed a PNR, or from what other countries. As a result, attempts at mediation have been unsuccessful. Most travellers cannot afford to bring a lawsuit, especially if it has to be brought in another country and language.

What is API or APIS data? How is it different from PNR data? The "Advance Passenger Information System" includes some data extracted from PNR's, and some other government-mandated data such as passport details. APIS data includes information that would be included on the passenger manifest, ticket, and passport, but also some additional information such as the complete itinerary (including flights that might have been separately ticketed). Since APIS data generally includes the PNR record locator, APIS data effectively gives the recipient the ability to obtain the entire PNR.

What is "Secure Flight Passenger Data"? How is it different from PNR or APIS data? "Secure Flight" is a scheme currently being deployed for making "fly/no-fly" decisions about passengers on domestic flights in the U.S. Like APIS data, "Secure Flight Passenger Data" (SFPD) includes some data extracted from PNR's, and some data that wouldn't otherwise be included in PNR's. Airlines are not required to include SFPD in PNR's, but in practice it is easier for them to include it in PNR's than to store it separately. The SFPD data set is slightly

different from the APIS data set, but includes some of the same elements such as the PNR record locator. The DHS plans to replace some of its current "fly/no-fly" decision-making systems for international flights with "Secure Flight". If this is implemented without withdrawing any current DHS requirements, that would mean that airlines operating international flights to or from the U.S. would have to transmit three partially redundant sets of data for each passenger: PNR, APIS, and SFPD.

How does the DHS store its copies of PNR and APIS data? Both PNR's and APIS records, or pointers to them, are stored in the DHS "Automated Targeting System" (ATS). ATS operated illegally for years, in violation of the U.S. Privacy Act, before the DHS published the required notice of its existence. No action has been taken to expunge the data collected illegally, or to discipline the responsible DHS officials.

Is PNR and APIS data used by DHS for profiling? Yes. The PNR, APIS, and other ATS data for each international passenger traveling to or from the U.S. is evaluated by a secret process using secret algorithms in secret lists, on the basis of which each passenger is assigned a risk score of "cleared", "inhibited", or "not cleared". This determines whether the airline is given permission to allow them to board, or whether the airline is directed to ask additional questions or contact local law enforcement.

Is PNR and APIS data used by DHS for data mining? Yes. In addition to mining PNR's for the data used in real time to determine whether to allow passengers to fly, the PNR's are mined for matches against other secret lists of data. According to the DHS, the purpose of this sort of data mining is to identifying new suspects, not to investigate people who were already under suspicion. For example, the presence of a phone number in your PNR matching a phone number in someone else's PNR might make you a suspect. That might be the phone number of a travel agent, or it might be the phone number of the hotel where you were staying when you reconfirmed your flight. But under the DHS "guilt by association" system, this phone number might subject you to search, surveillance, questioning, or denial of permission to travel.

Is there any U.S. law that guarantees that no-fly decisions based on PNR data will be consistent with internationally recognized human rights? No. The the right to freedom of movement is guaranteed by Article 12 of the International Covenant on Civil and Political Rights (ICCPR). The U.S. ratified the ICCPR with the reservation that it is not "self-executing" in the U.S., and has never adopted any specific implementing legislation. As a result, the ICCPR cannot in itself be a cause of action in any U.S. court.

Has the DHS evaluated its demand for PNR data against the standards applicable under international treaties for measures that burden the exercise of fundamental rights? No. The standards for evaluating measures that implicate the right to freedom of movement under Article 12 of the ICCPR were established by the U.N. Human Rights Committee in its *General Comment No. 27: Freedom of Movement*. The DHS has never evaluated any of its regulations with respect to the ICCPR or these standards.

Does the DHS have any designated point of contact or procedures for responding to

complaints of violations of human rights, including the right to freedom of movement? No. The DHS has received such complaints, but has not responded to them.

Has the DHS allowed judicial review of no-fly decisions based on PNR data? No. No legal challenge to the validity of a no-fly decision has gone to trial. The DHS has actively resisted, and continues to resist, allowing any such lawsuit to go to trial. Former Secretary of Homeland Security Chertoff said of no-fly decisions, "We don't conduct court hearings on this." The current Secretary has announced no change in this position.

Would the proposed PNR "agreement" be binding on the DHS or other US government agencies? No. Under the U.S. Constitution, the only binding international instruments are treaties ratified by a two thirds vote of the U.S. Senate. The DHS has no authority to bind the U.S. to any agreement without its ratification by the Senate as a treaty. The proposed PNR agreement could not be enforced by any U.S. court.

Would the proposed PNR agreement be subject to judicial review in the U.S.? No.

What recourse would travelers or other data subjects have under U.S. law if the DHS violated the proposed PNR agreement? None.

Do DHS policies provide for subject access to complete PNR's or other data used as the basis for no-fly decisions? No. In February 2010 the DHS promulgated a new rule exempting much of the personal data in the Automated Targeting System, including large portions of PNR's, from disclosure in response to subject access requests. At the same time, the DHS indicated its intent to continue to collect and retain this secret data, and to rely on it in making no-fly decisions. The portions of PNR's to be kept secret from data subjects would include information provided by travel companies, which is exactly the sort of information that is likely to be entered in PNR's without the travelers' knowledge.

Do DHS policies require the data used as the basis for no-fly decisions to be accurate, relevant, Were disclosed to travelers? No. The same February 2010 DHS rulemaking exempted the Automated Targeting System and the DHS database of PNR's from any U.S. legal requirement of accuracy or relevance, and from the requirement that data be collected, where possible, directly from the data subject. The DHS said that the purpose of the new rule was to enable the DHS to make decisions about whether to permit travelers to fly on the basis of information from third parties, without revealing that derogatory information or its source to travelers themselves.

What happens when a data subject requests their PNR's from the DHS? Typically, the DHS takes months or years to respond, if it responds at all. For example, one MEP received no response at all to their request for their PNR data until after they filed a lawsuit against the DHS in U.S. Federal court. Some requests are probably lost, and many requesters never receive any answer. Subject access requests must be made by mail. The DHS moved office and changed the address for PNR requests more than two years ago, but still has not published a new notice in the *Federal Register* with the correct address. So any requests sent to the address in the most recent official notice are returned as undeliverable. The DHS also

sends all its mail to a remote screening center before it is delivered to DHS offices, making it impossible to verify whether a request has actually been received by the proper office. The DHS does not publish any statistics on processing times for Privacy Act requests or appeals, on the percentage of such requests and appeals granted or denied, were on the backlogs of such requests or appeals. The last time the DHS Privacy Office reported on this issue, they said that requests for PNR data have typically taken more than a year to to answer.

When the DHS responds to a request for PNR data, what information do they typically provide? According to the Identity Project (PapersPlease.org), which has provided templates for PNR access requests and has reviewed the largest number of DHS responses, *all* of the responses they have reviewed have been incomplete, with information improperly withheld. If the DHS responds at all, they typically send a few PNR's for some of the requesters most recent trips to the U.S. (not all of their PNR's), and a summary index of other DHS records (each line of which typically corresponds to a page of notes which are not provided). Only PNR's for the data subject's own trips are provided, even if there is also personal data about the requester in PNR's for other travellers, such as other people whose tickets the requester paid for. Without specialized expertise in PNR, it's impossible to tell that this typical response is incomplete, what is missing, or how to interpret the partial data that is provided. Often it appears that the DHS censors don't understand the codes in the PNR's and other records they are censoring: their censorship is inconsistent or clearly improper. For example, a remark inserted by a travel agent in the PNR of an MEP (without the MEP's knowledge), identifying the traveller as an MEP, was blacked out in the copy of the PNR that was released by the DHS, but not redacted from the “history” (change log) released along with the PNR. Similarly, requesters' own phone numbers or contact information have been blacked out in the redacted copies of their PNR's released by the DHS.

What can a data subject do if they receive no answer from the DHS to a request for their PNR data, or an incomplete or improperly redacted answer? They can file an administrative appeal with the same division of the DHS that responded (or didn't respond) to their original request, or they can hire a U.S. lawyer and file a lawsuit in U.S. Federal court. Some Privacy Act appeals related to PNR access requests have been ignored by the DHS for more than two years. A Federal lawsuit costs at least tens of thousands of U.S. dollars, and typically takes at least one to two years, often longer. The DHS has vigorously contested lawsuits related to PNR data. Even in the cases that have been litigated, data subjects have still received only incomplete and redacted PNR data.

What about the DHS “TRIPS” program? Is it an appeal or oversight program? Not really. The TRIPS program operates entirely in secret and involves “review” by the same agencies that made the original decision. Since someone who makes a request for “redress” under TRIPS is never told the basis of the original decision, and never sees the evidence (if any) against them, they can only guess at what evidence to submit that might cause the secret decision-makers to reverse themselves. The requester doesn't have a hearing and is never told what, if any, action has been taken in response to their request. The only way to find out if the secret decision has changed is to buy another ticket, and try to fly again. TRIPS decisions cannot be reviewed by any U.S. court.

Has there been any independent review of DHS compliance with the PNR agreement? No. U.S. government agencies such as the General Accountability Office and the DHS Inspector General have reviewed DHS compliance with U.S. law. But since the DHS agreement with the EU on PNR is not part of U.S. law and not legally binding they have not reviewed compliance with that agreement. The only review of compliance with the agreement on the U.S. side was conducted in secret by the DHS Privacy Office – the same office that is responsible for responding to Privacy Act subject access requests. The DHS has not disclosed who participated on the U.S. side in the joint DHS-EU reviews, but it does not appear that they included any independent technical experts.

Has analysis of PNR data detected some terrorists? We don't know. Some people have been refused permission to fly, or refused permission to enter the U.S. But none of these no-fly decisions or denials of admission to the U.S. has been reviewed by any court.

Could the DHS have obtained these PNR's through a court order or normal law enforcement procedures, without the PNR agreement? Probably, but we don't know. There is no public record that the DHS has ever tried to go through normal legal procedures or get a court order for access to PNR, in the U.S. or any other country.

Have some people been kept off planes because of data in PNR's? Yes. The U.S. has arrested innocent people, tortured innocent people, and sent innocent people to Guantanamo. The DHS only talks about a few examples from among a much larger number of people who have been kept off planes. We don't know how many of the people kept off planes have been terrorists, and how many have been innocent people falsely placed under suspicion and deprived of their right to freedom of movement.

Has analysis of PNR data detected some other crimes? Yes, of course. If you watch everyone all the time, you will see some crimes. If you break into every house and search inside, you will find some contraband. Does this mean that we should have universal surveillance and warrantless searches, and that everyone should be treated as a criminal suspect when they want to exercise their fundamental right to travel?

What sort of people are kept off flights or kept out of the U.S. on the basis of PNR data? The only no-fly case pending in U.S. courts involves a university professor who had lived legally in the U.S. for years. She has been charged with no crime, but she was refused permission to fly and then refused permission to return to the U.S. After years of litigation, the DHS still refuses to show her any of the evidence (if any) against her, tell her what (if anything) she is accused of doing or why she is not allowed to fly, or tell her who or what agency is responsible for putting her on the no-fly list.

What will happen if the EP rejects the proposed PNR agreement with the DHS? For U.S. government agencies will be able to obtain PNR data through normal legal procedures and existing law enforcement cooperation agreements.