

**Before the
European Commission
Directorate-General for Energy and Transport
Office DM24 5/98
B-1049 Brussels
BELGIUM**

TREN-CONSULTATION-CRS@ec.europa.eu

Public consultation:

Possible revision of Regulation 2299/89 on a
Code of Conduct for Computerised Reservation
Systems (CRS)

**COMMENTS OF
THE IDENTITY PROJECT (IDP)
AND JOHN GILMORE**

The Identity Project (IDP)

<<http://www.PapersPlease.org>>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

USA

The Identity Project submits these comments in response to the Commission's notice at http://ec.europa.eu/transport/air_portal/consultation/2007_04_27_en.htm, and the "Consultation Paper on the Possible Revision of Regulation 2299/89 on a Code of Conduct for Computerised Reservation Systems (CRS), available at http://ec.europa.eu/transport/air_portal/consultation/doc/2007_04_27/2207_04_27_crs_consultation_paper_en.pdf.

These comments are not confidential, and may be published by the Commission.

These comments are in response to Question 1 of the Consultation Paper: "[I]s there still a need for the sector-specific competition rules imposed by the Code of Conduct? Or should the Code of Conduct be revised or abolished?"

The Identity Project believes that the rules in the Code of Conduct for CRSs related to the processing and disclosure of personal information contained in reservations are still needed. These provisions of the Code of Conduct for CRSs should be retained, strengthened, and enforced.

I. ABOUT THE IDENTITY PROJECT

The Identity Project (IDP), <<http://www.PapersPlease.org>>, provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit nongovernmental organization, incorporated under the laws of the state of California, providing legal and educational resources dedicated to protecting and promoting human rights under the First Amendment to the U.S. Constitution and similar provisions of other national and international laws.

II. THE RULES IN THE CODE OF CONDUCT RELATED TO PROCESSING AND DISCLOSURE OF PERSONAL INFORMATION SHOULD BE RETAINED.

Clearly, personal data contained in Passenger Name Records (PNRs), customer profiles, and other records collected, stored, or processed by CRSs should be protected. And this personal data is protected by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 , 23.11.1995, p. 31 - 50).

But neither data subjects nor data protection authorities can readily determine if the travel agency, the CRS, or the airline is the "data controller" for PNRs, customer profiles, or other personal data collected, stored, and processed by CRSs. As a result of this uncertainty, violations of the Data Protection Directive could, and often do, evade enforcement. The data protection rules in Article 6, Article 9a, and Article 10 of the Code of Conduct for CRSs (attached as an Appendix to these comments) are needed to ensure that personal data in PNRs, customer profiles, and other CRS records is adequately protected, regardless of which entity is considered the "data controller".

Most travellers are unaware of the existence of CRSs. Travellers have no direct contact with CRSs, and no way to know to which CRS(s) their data has been disclosed. Travellers' rights under the

Data Protection Directive would be meaningless without the requirements of Article 9a and Article 10 of the Code of Conduct for CRSs that system users identify the CRS(s) to the traveller on request.

Travellers need to know which CRS(s) will be used to store or process their personal data, in order to know if their data will be transferred outside of the European Union. Three of the four largest CRSs (Sabre, Galileo, and Worldspan) are based in the United States. The fourth (Amadeus) operates a major PNR aggregation, warehousing and processing division in the U.S. (Amadeus Revenue Integrity, formerly Airline Automation, Inc.).

Once personal data is transferred to any of these CRSs, it could be accessed by the U.S. government, other governments, or other commercial entities in the U.S. or other countries.

The Commission should keep in mind, in its consideration of whether to revise or repeal the provisions of the Code of Conduct for CRSs related to personal data, that no data protection law or regulation that governs CRSs in the U.S. Under U.S. law, personal data obtained by a CRS or other commercial entity is considered the exclusive property of that entity, in which the data subject has no rights. Once the data is transferred to the U.S., the CRS or other entity can give or sell that data to any government, commercial, or other entity, anywhere in the world, without the knowledge or consent of the data subject. This can happen as soon as a European travel agency or tour operator creates a customer profile or PNR in Sabre, Galileo, or Worldspan; or as soon as a PNR is transferred to Amadeus Revenue Integrity for processing. The CRS is not required by U.S. law to allow the data subject to access their own data, and the CRS is not required to tell the data subject to whom their data has been provided.

The Commission should also keep in mind that the so-called "agreement" or "undertakings" of the U.S. Department of Homeland Security (DHS), Bureau of Customs and Border Protection (CBP) regarding access to PNR data by the CBP are limited to "the PNR data which CBP accesses (or receives) directly from the air carrier's reservation systems for purposes of identifying potential subjects for border examination". Data obtained from other sources, by other agencies (or any other commercial or government entities), or for other purposes is not protected by the CBP undertakings.

For example, data obtained from the travel agency's or tour operator's CRS rather than the airline's CRS, data obtained from a PNR processor such as Amadeus Revenue Integrity rather than the airline's host CRS, data obtained by any U.S. government agency other than through the CBP (including the FBI, NSA, or other DHS divisions), and data obtained by the CBP for other purposes is not protected.

Once data is transferred to a CRS or other entity in the U.S., it can be accessed by the U.S. government, other governments worldwide, or other commercial entities or individuals, without the knowledge or consent of the data subject, the travel agency or tour operator that collected the data, or the airline. Orders from the U.S. government to a CRS or other entity or individual, directing them to disclose personal data originally collected in the European Union (or anywhere else) can forbid the recipients of those orders from disclosing those orders to the data subject, the entity in the E.U. from which the data was received, or anyone else. Thus, as soon as data is transferred to a CRS in the U.S., it can be further transferred without the knowledge or consent of the airline or the data subject, and the CRS could be compelled by U.S. government order to conceal those disclosures.

In addition, the CBP undertakings are unilateral, nonbinding, and by their own explicit terms grant data subjects no enforceable legal rights. Since they have not been enacted into U.S. law, promulgated as a U.S. Federal agency regulation, or ratified by the U.S. Senate as a treaty, the CBP undertakings cannot provide a legal cause of action or be invoked as legally binding in any U.S. court.

The Commission should therefore recognize the insufficiency of the CBP undertakings, the lack of adequate protection for government data in the U.S., the lack of any data protection for commercial data in the U.S., and the continued need for the data protection rules in the Code of Conduct for CRSs.

III. THE RULES IN THE CODE OF CONDUCT RELATED TO PROCESSING AND DISCLOSURE OF PERSONAL INFORMATION SHOULD BE STRENGTHENED TO INCLUDE PROTECTION FOR DATA SUBJECTS OTHER THAN PASSENGERS.

Article 6 of the Code of Conduct protects personal information concerning passengers, and, in part, corporate users:

1. The following provisions shall govern the availability of information, statistical or otherwise, by a system vendor from its CRS: ... (b) any marketing, booking and sales data made available shall be on the basis that: ... (ii) such data ... shall include no identification, either directly or indirectly, of, or personal information on a passenger or a corporate user; ...
2. A system vendor shall not make personal information concerning a passenger available to others not involved in the transaction without the consent of the passenger.

These sections of the Code of Conduct should not be limited to passengers or corporate users.

All subjects of data collected, stored, or processed by CRSs should receive the same level of protection.

In addition to data concerning passengers, PNRs and customer profiles processed by CRSs contain personal data concerning the following categories of individuals, among others:

- A. Travel arrangers, personal assistants and administrative staff, travel managers, group coordinators, event organizers, and family members and friends assisting with travel arrangements, as identified by the “received from” field in each PNR that records the person who requested the creation of the reservation or the most recent change to it, and from contact information in customer profiles.
- B. People who pay for tickets for others, or who hold joint credit or debit cards with people who purchase travel for themselves or others – whether or not they travel themselves – as identified from the “form of payment” fields in ticketing records in PNRs and profiles.
- C. Friends, family members, hosts, housemates, domestic partners, and business associates of travellers, as identified from the "local contact" and "document delivery" information in PNRs and profiles (which may include phone numbers, descriptions of the relationship of the contact to the traveller, and in some cases addresses).
- D. Travel industry personnel, including travel agents and airline reservation, check-in, and ticketing staff, as identified by the unique “agent sine” or log-in ID in each PNR and by the city or “pseudo-city” (airline office or travel agency branch or location) and the LNIATA or “set address” of the terminal or data connection on which the entry was made (the CRS or airline hosting system counterpart of an Internet IP address).
- E. Clients, customers, and employers of travellers, even if they aren’t travelling, as identified by billing and accounting codes for travel by others undertaken on their behalf or at their expense. Corporate travel agencies routinely include codes in PNRs to indicate to the traveller (or the traveller’s employer) to which department, project, or client the cost of the trip is to be billed. In the case of a law firm, these entries routinely identify the specific client, case, or matter on whose behalf or at whose expense the travel was undertaken. Thus clients of law firms, consultants, financial advisors, and other

professionals are routinely the subject of data in PNRs, and thus could be the subject of data (including legally privileged and sensitive data) processed by CRSs.

All of these categories of individuals deserve the same data protection as passengers. Article 6, Section 1(b)(2) and Article 6, Section 2 of the Code of Conduct should be amended to replace the references to "passenger", as quoted above, with "individual data subject".

IV. THE RULES IN THE CODE OF CONDUCT RELATED TO PROCESSING AND DISCLOSURE OF PERSONAL INFORMATION SHOULD BE ENFORCED.

Both the Data Protection Directive and the data protection provisions of the Code of Conduct for CRSs are routinely, systematically, and flagrantly violated. The Identity Project requests that the Commission immediately initiate investigations and enforcement proceedings against CRSs – including Sabre, Galileo, Worldspan, and Amadeus Revenue Integrity -- for violations of the Code of Conduct.

Whenever a travel agency, tour operator, or airline creates a PNR or customer profile in Sabre, Galileo, or Worldspan; or when data from an Amadeus PNR is accessed by Sabre, Galileo, Worldspan, Amadeus Revenue Integrity, or any U.S. government agency; personal data is transferred from the territory of the E.U. to the U.S., where it is not adequately protected. Each of these transfers is in violation of the Data Protection Directive, which prohibits transfers of personal data to countries outside the E.U. where that data is not adequately protected. And unless the consent of the passenger is obtained for each such transfer of personal data, the Code of Conduct for CRSs is also violated. Those violations occur regardless of the CBP undertakings, and even if the U.S. government does not access the data.

We know of no travel agency, tour operator, or airline in the E.U. which discloses to its customers that its use of a CRS which stores or processes PNRs in the U.S. will involve the transfer of personal data to the U.S., or obtains the consent of passengers or other data subjects for these transfers.

Customers and other subjects of personal data collected and transferred to CRSs in the U.S. by these travel companies are properly entitled by the Data Protection Directive and the Code of Conduct for CRSs to notice and an opportunity to consent, before these transfers occur. Most travellers do not know about these transfers, and would not consent to them. We urge the Commission to protect their rights by taking action, as soon as possible, to bring the CRSs into compliance with E.U. laws.

Respectfully submitted,

The Identity Project (IDP)

<<http://www.PapersPlease.org>>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

USA

_____/s/_____

Edward Hasbrouck,

Consultant to IDP on travel-related issues

James P. Harrison

Staff Attorney, First Amendment Project

Director, IDP

John Gilmore

Post Office Box 170608

San Francisco, CA 94117

USA

27 April 2007

Council Regulation (EEC) No. 2299/89 of 24 July 1989 on a code of conduct for computerized reservation systems (OJ L 220, 29.7.1989, p. 1)

as amended by:

**Council Regulation (EEC) No. 3089/93 of 29 October 1993 (OJ L 278, 11.11.1993, p. 1)
and Council Regulation (EC) No. 323/1999 of 8 February 1999 (OJ L 40, 13.2.1999, p. 1)**

and as corrected by:

Corrigendum, OJ L 17, 25.1.1995, p. 18 (3089/93)

... Article 6

1. The following provisions shall govern the availability of information, statistical or otherwise, by a system vendor from its CRS:

(a) information concerning identifiable individual bookings shall be provided on an equal basis and only to the air carrier or carriers participating in the service covered by and to the subscribers involved in the booking. Information under the control of the system vendor concerning identifiable individual bookings shall be archived off-line within seventy-two hours of the completion of the last element in the individual booking and destroyed within three years. Access to such data shall be allowed only for billing-dispute reasons.

(b) any marketing, booking and sales data made available shall be on the basis that: ...

(ii) such data ... shall include no identification, either directly or indirectly, of, or personal information on a passenger or a corporate user; ...

2. A system vendor shall not make personal information concerning a passenger available to others not involved in the transaction without the consent of the passenger.

3. A system vendor shall ensure that the provisions in paragraphs 1 and 2 above are complied with, by technical means and/or appropriate safeguards regarding at least software, in such a way that information provided by or created for air carriers can in no way be accessed by one or more of the parent carriers except as permitted by this Article...

Article 9a

1. ... (d) ... The subscriber shall inform the consumer of the name and address of the system vendor, the purposes of the processing, the duration of the retention of individual data and the means available to the data subject of exercising his access rights.

(e) A consumer shall be entitled at any time to have a print-out of the CRS display or to be given access to a parallel CRS display reflecting the image that is being displayed to the subscriber.

(f) A person shall be entitled to have effective access free of charge to his own data regardless of whether the data is stored by the CRS or by the subscriber....

Article 10 ...

2. A system vendor shall, on request, provide interested parties, including consumers, with details of current procedures, fees and system facilities, including interfaces, editing and display criteria used. For consumers that information shall be free of charge and cover the processing of individual data. This provision shall not, however, require a system vendor to disclose proprietary information such as software.