

**COMMENTS OF
INTERNATIONAL AIR TRANSPORT ASSOCIATION**

IN RESPECT TO:

**US Customs Service Interim Rule on
Passenger Name Record Information Required for Passengers on Flights
in Foreign Air Transportation to or From the United States**

**19 CFR Part 122
RIN 1515 -AD06
(42710 Federal Register/ Vol. 67, No. 122, of 25 June 2002)**

August 26, 2002

Robert A. Davidson
IATA Assistant Director, Facilitation Services
800 Place Victoria
P.O. Box 113, Montreal, Quebec, Canada H4Z 1M1
514.874.0202

David M. O'Connor
IATA Director, United States
1776 K St. N.W. Suite 400
Washington, D.C. 20006
202.293.9292

**COMMENTS OF
INTERNATIONAL AIR TRANSPORT ASSOCIATION**

IN RESPECT TO:

**US Customs Service Interim Rule on
Passenger Name Record Information Required for Passengers on Flights in Foreign
Air Transportation to or From the United States**

**19 CFR Part 122
RIN 1515 -AD06
(42710 Federal Register/ Vol. 67, No. 122, of 25 June 2002)**

On behalf of its 274 member airlines, ninety-four of which provide scheduled international air services to the United States, the International Air Transport Association (IATA) is pleased to be given this opportunity to provide comments concerning the interim rule referred to above.

The aviation industry, in particular, recognises that safety of flight, airport security and national border integrity, in great part, depend upon an improved level of information exchange between all parties involved. Airlines serving the U.S. market have clearly demonstrated their ability to work cooperatively with the authorities by providing Advance Passenger Information (API) data at proficiency levels many thought were not achievable in such a short time frame. These same airlines, both individually and through various trade associations, have joined with the U.S. Customs Service and other interested governmental agencies in identifying and developing other automated solutions to meet today's new requirements.

Now, with enactment of various Federal laws (including Public Law 107-71), a significant expansion of access to private consumer information is sought – namely data contained within airlines' reservation and departure control systems (DCS). In the aftermath of the tragic events of September 11th, the airline industry understands and can well appreciate the reasoning behind Congress' mandate. However, there are several critical issues that will need to be addressed and resolved before this program can be implemented in a manner that won't impose conflicting compliance obligations on the affected airlines. We believe that a number of steps must be taken to ensure that airlines are not forced to violate the laws of their own or other countries which they serve, and thereby compromise protections afforded their customers in such countries, in order to comply with this new U.S. requirement.

Our comments will not be extensive, but we do wish to address several areas of concern to the airline industry raised by the interim rule. These include 1) existing inter-

governmental accords controlling electronic exchange of personal data, 2) specific national laws on data privacy, and 3) a carrier's legitimate need to safeguard legacy systems and protect proprietary commercial information from misuse.

General Comments

First and foremost, all airlines serving the United States are concerned that allowing blanket, unfettered access, by a multitude of governmental agencies, may violate data privacy laws imposed by States to protect the interests of their own nationals. Airlines are not only subject to their own national legislation but also to the data protection laws of any country in which they operate. In some countries, such as Colombia and Israel, violation of data privacy laws may result in criminal prosecution and civil liability. Data privacy issues have, of course, arisen in the context of Advance Passenger Information (API). However, in the case of API, the data elements are very specific, directly related to the passenger's entry into the United States. The elements can be explained to and approved by the traveller as required. For the most part, these are data elements that are carried in the traveller's passport or are voluntarily provided to the authorities (INS or Customs) upon arrival in the U.S.

In that regard, API stands in stark contrast to the information stored in airline reservation systems, since the range of data that are contained in individual Passenger Name Records (PNRs) varies significantly from airline to airline. Indeed, much of the data contained in these records (e.g. special dietary needs, mobility or medical conditions, or credit card information) does not necessarily relate to the individual's specific flight to the United States and therefore may fall outside the scope of the requirements laid out in Public Law 107-71 and in its implementing regulations as contained in this interim rule. In particular, special dietary requirements may be linked to religious beliefs and therefore be considered as "sensitive data" under various data protection laws. Accordingly, a thorough evaluation of the impact of these regulations, in light of current data privacy laws and special concerns for sensitive data, should be undertaken.

In most instances, a carrier's ability to comply with the Service's access requirements will be based upon political decisions taken both in Washington DC and in various national capitals around the world. This will require an active dialogue between representatives of the Treasury Department (supported by the U.S. Departments of Transportation and State) and appropriate ministries and Data Privacy Authorities (where they have been established) in the various States.

Specific guidance materials have been developed both within the United States and in the European Commission that may help to resolve many of the more problematic issues. These will be discussed in detail later.

EC Data Protection Directive (95/46/EC)¹

This Directive, binding on all 15 current EU member states and those that will join the Community in the future, restricts the transfer of data to a third country except when certain conditions are met. Specifically, this Directive requires that the receiving State must have adequate measures in place to protect personal data that meet minimum requirements. Further, the Directive requires that the rightful owners of the data in question be fully informed of the nature of and purpose for the data that is to be transferred. Where sensitive data is involved, the owner of the data must actively consent to its transmission to any third party.

The EC Directive serves as the foundation for all individual European States' Data Privacy legislation. In response, and to reduce opposition by various States to the transfer of data to U.S. agencies, the US Department of Commerce, through its Safe Harbour Privacy Principles (21 July 2000), developed specific guidelines on personal data protection measures. These have received official EU recognition², and their adoption by the Service would go far in reducing concerns that many States and many airlines have in connection with access to reservation systems. As another option under the Commission's decision, government agencies may develop and implement their own self-regulatory privacy policies, provided that they conform to the already-approved Principles.

Should Customs adopt the Safe Harbour Privacy Principles, an additional issue will need to be resolved. In the interim rule, the Service advises that data obtained through PNR access may, upon request, be shared with other Federal agencies for the purpose of protecting national security. This is problematic, both under national and Community legislation, in that data that is collected and transferred to another party may be used only for the purpose for which it has been collected. As a consequence, even if Customs were to avail itself of the Safe Harbour mechanism, transferring this data to other US agencies would require that each receiving agency similarly undertake to self-certify under the "Safe Harbour" principles established by Commerce and ratified by the European Commission, or implement their own conforming self-regulatory privacy policies. While not insurmountable, such data sharing between the Service and other U.S. agencies will add significantly to the complexity of the process, and to the solutions and/or guarantees that will be required.

National Data Privacy Legislation

In preparing to draft these comments, IATA requested information from its members concerning existing national laws protecting data privacy, as well as actions that might be taken to overcome legal obstacles to carriers' compliance with the Service's PNR access requirement. In most of the responses received to date, carriers indicated that their countries had implemented national legislation to control the exchange of personal data

¹ 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.

² Commission Decision 2000/520/EC, 26 July 2000

with third parties – including foreign governments or their agencies. In some cases, such as Switzerland, such legislation can be very prescriptive as to the guarantees and technical features imposed on data collectors where they intend to transmit data abroad³. Within the European context, most legislation has been drafted in accordance with the European Commission’s Directive referred to in the previous section.

Specifically, respondents referred to the following national laws:

Colombia:	Article 15, Colombian Constitution
Czech Rep:	Act no 101/2000 on the Protection of Personal Data
Greece:	Law 2472/1997 ⁴
Israel:	Protection of Privacy Law
Mexico:	Article 122: Ley de Vías Generales de Comunicación
Philippines:	Bill of Rights, Article III, Sections 2 and 3, Civil Code, Article 32,
Spain:	Data Protection Law (15/1999) ⁵
Sweden:	Personal Data Act (1998: 204, Sections 33, 34 and 35) ⁶
Switzerland:	Data Protection Act (DSG; SR 235.1, of 19 June 2002), and Art. 139 I lit a., Swiss Private International Law Code

In each of these instances, the laws strictly control the exchange of personal data between a commercial entity and a foreign entity (commercial or governmental). In all cases, the laws require that the receiver of this data maintain an adequate level of protection, and that the owner of the data approves its transfer. We believe that by adopting the “Safe Harbour” principles and self-certifying compliance with the terms of the Commerce Departments guidelines, the Service will be in a position to overcome many concerns raised by foreign governments. Alternatively, the Service could publish its own self-regulatory privacy policy along the lines of the Safe Harbour Principles.

To comply fully with the requirements under the legislation cited above, Customs would need to have its self-certification officially recognised and communicated to the appropriate Ministries, and where they exist, Data Privacy Authorities in the various countries of origin.

Safeguarding Legacy Systems and Protecting Proprietary Commercial Information

The interim rule also sets forth the requirement that airlines provide it with an electronic connection to their reservation or departure control systems. In any situation where two systems are linked, opportunities are created by which persons with malicious intent can gain access through the portals created to facilitate exchange and 1) damage or disable the accessed system, or 2) illegally obtain information of sensitive personal or commercial nature. We believe that the worthy goal of enhanced national security afforded by carriers’ cooperation in this process should include safeguards by Customs

³ IATA understands Swiss International Airlines intends to file specific comments describing this in detail.

⁴ This Act incorporates the EC Directive on Processing of Personal Data (95/46/EC) into Greek Law

⁵ This Act incorporates the EC Directive on Processing of Personal Data (95/46/EC) into Spanish Law.

⁶ This Act incorporates the EC Directive on Processing of Personal Data (95/46/EC) into Swedish Law

ensuring that the carriers' legacy systems and the data that they contain are protected from illegal outside access.

The interim rule, while requiring carriers to provide access, does not place regulatory limits on that access by Service systems. We believe that it is critical that the final rule state clearly and unequivocally that access to airline systems shall be limited to "read only" capabilities. Further, the final rule must state that Customs does not have the authority to access and shall not access records of any flight that does not originate from or terminate in U.S. territory. This second provision is essential for any carrier whose reservation or DCS system contains both foreign to/from foreign and foreign to/from U.S. flight records. Absent such guarantees, many carriers would be forced to seek permission to provide the U.S. authorities access to reservation and/or manifest data even for passengers not travelling to or from the United States. This clearly goes far beyond the scope of the legislation.

The final rule should also exclude Service access to carrier's commercially sensitive frequent traveller databases in specific terms, as those databases are not specified in Public Law 107-71.

Conclusions

Gaining approval from various governments for providing Customs with access to airline systems will likely prove to be a complex and time-consuming process in many instances, particularly in those countries that have implemented vigorous data privacy laws consistent with the European Community's Directive. Therefore, it is imperative that Customs, in cooperation with Commerce and the Department of State, initiate immediate consultations with the appropriate Ministries of those countries. This will help to ensure that carriers are not forced to choose between the lesser of two evils – violating national legislation or being forced to withdraw from service to the U.S.

We firmly believe that many current obstacles will be overcome provided Customs undertakes, as part of the final rule, to:

- self-certify under the Department of Commerce "Safe Harbour" Principles or develop and implement self-regulatory data privacy policies that conform to those Principles;
- communicate that self-certification or privacy policy development to all governments having data privacy legislation adopted in accordance with the EU Directive;
- provide guarantees that limit sharing of data obtained through access to airline systems only to those agencies that have self-certified under, or fully adopted the "Safe Harbour" principles;
- limit its access to "read only" capability and provides assistance in blocking illegal outside access; and,
- provide assurances to governments and to carriers alike that it will limit access to information pertaining only to those flights touching U.S. territory.

As stated at the outset of this submission, the issues surrounding data protection and system access are largely political in nature, and will require appropriate political dialogue between governments to be resolved. While the airline industry is readily prepared to provide technical expertise in connecting computer systems, it is far less equipped to answer the legal and policy questions posed by the interim rule which are perhaps better suited for resolution at the ministerial level.

In light of the foregoing, we strongly encourage Customs to initiate such necessary discussions with the appropriate Data Privacy Authorities and Ministries prior to imposing sanctions, monetary or otherwise, against any carrier that has not satisfied an outstanding or prospective request for system access. The International Air Transport Association is fully prepared to offer any assistance possible to further this process and ultimately, to protect the interests of Customs, our members and the travelling public.

Respectfully submitted by:

Robert A. Davidson
Assistant Director, Facilitation Services
International Air Transport Association
Montreal, Quebec, Canada H4Z 1M1

26 August 2002