Advance Passenger Information/ Passenger Name Record: Privacy Rights and Security Awareness

By Nicolas Paul Banerjea-Brodeur
Faculty of Law, Institute of Air & Space Law
July 2003

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the LL.M degree

McGill University, Montreal

Your file Votre référence
ISBN: 0-612-98774-4
Our file Notre référence
ISBN: 0-612-98774-4

Disclaimer

All views and opinions expressed in this thesis are those of the author alone and do not necessarily reflect those of any other individual, the International Civil Aviation Organization, IATA, or any other government agency or air carrier.

Table of Contents

Disclaimer.....ii

Abstract.....vi

Acknowledgements.....x

Introduction.....11

Chapter 1 Advance Passenger Information and Passenger Name Record.....15

1. Advance Passenger Information.....15

1.1 Definition.....15

1.2 Legal Foundation for API.....17

1.3 History of *Annex 9* SARPS.....19

1.4 Advance Passenger Information Guidelines.....24

2. Passenger Name Record.....29

3. Contracting States Applications of API and PNR.....30

3.1 The United States of America.....30

3.2 The Canadian Position.....43

3.3 The United Kingdom Position.....47

3.4 Initiative of the Kingdom of Spain.....49

3.5 The Australian Position.....50

3.6 The German and Swiss Positions.....52

3.7 The Mexican Approach.....53

3.8 Republic of Korea.....54

4. Conclusion.....54

Chapter 2: The Understanding of Machine Readable Travel Documents and Biometric Procedures.....57

1. Machine Readable Travel Documents.....57

1.1 Definition.....57

1.2 Historical Background of MRTDs.....58

1.3 Legal Foundation for MRTDs.....59

1.4 MRTD Objectives.....59

2. Biometric Procedures.....61

2.1 Limitations.....62

2.2 Legal Foundation.....63

2.3 Type of Biometric Procedures.....64

2.4 Problems to Be Encountered by Biometric Procedures.....75

Chapter 3: Privacy Rights Towards Advance Passenger Information/ Passenger Name Record.....77

1 Passenger Rights.....78

2 Legal Foundation for Collection of Data.....81

3.The Concept of Privacy and "Reasonable Expectation".....82

4 European Position.....86

5 The "National Security" Justification.....88

6 Physical Characteristics and the Right of Privacy.....90

7 Privacy Rights vs US APIS System.....92

Conclusion.....96

Bibliography.....98

ABSTRACT

An in-depth study of Advance Passenger Information and Passenger Name Record has never been accomplished prior to the events of September 11th. It is of great importance to distinguish both of these concepts as they entail different legal consequence. API is to be understood as a data transmission that Border Control Authorities possess in advance in order to facilitate the movements of passengers. It is furthermore imperative that harmonization and inter-operability between States be achieved in order for this system to work. Although the obligations seem to appear for air carriers to be extraneous, the positive impact is greater than the downfalls.

Passenger Name Record access permits authorities to have additional data that could identify individuals requiring more questioning prior to border control clearance. This data does not cause in itself privacy issues other than perhaps the potential retention and manipulation of information that Border Control Authorities may acquire. In essence, bilateral agreements between governments should be sought in order to protect national legislation.

The common goal of the airline industry is to ensure safe and efficient air transport. API and PNR should be viewed as formalities that can facilitate border control clearance and prevent the entrance of potentially high-risk individuals.

ABSTRACT

L'étude du dossier de renseignements obtenus au préalable de passagers ainsi que celui du dossier de réservation n'a jamais été amorcée en détail étant donné les évènements récents du 11 septembre. Afin de bien comprendre ces deux principes, il est impératif de les étudier séparément car ils possèdent différentes conséquences juridiques.

Le dossier de renseignements de passagers est transmis aux différentes autorités douanières afin de faciliter le trafic des passagers. Pour que ce système fonctionne, Il est de plus important de créer une uniformité globale afin d'obtenir une industrie du transport où les intervenants peuvent coopérer et y légiférer de façon standardisée. Enfin, il faudrait considérer de manière positive ce processus malgré le fardeau que cela impose aux transporteurs aériens, si ce n'est que de par son objectif premier.

En ce qui concerne le dossier de réservation des passagers, l'information accédée pourrait plutôt servir à identifier les individus requérant des formalités additionnelles aux frontières. Cette information comme telle ne créée pas de violation au droit à la vie privée si ce n'est que de la possible manipulation ou rétention illégale de données par les autorités. Pour s'assurer d'un système sécuritaire, les gouvernements devraient plutôt rechercher à conclure des accords bilatéraux afin d'empêcher toute violation possible à sa propre loi nationale.

L'industrie du transport aérien a un but commun : celui d'assurer le transport de manière efficace et sécuritaire d'un point à un autre. Ces données devraient être perçues comme des formalités permettant un accès efficace à la frontière tout en empêchant l'individu à risque de pénétrer à l'intérieur d'un État.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the assistance of my parents and my sister, who have permitted me to acquire the education and knowledge that I possess today. I also wish to thank God for his continuous support.

I wish to also thank my supervisor, Dr. Michael Milde, whom has encouraged me prior to my admission at McGill University and has always supported my accomplishments and career objectives.

I also would like to express my appreciation to the International Air Transport Association and more specifically to Mrs. Constance O'Keefe, Mr. Robert A. Davidson and Mrs. Georgina Graham for their valuable contribution to the advancement of my thesis.

The following will be an extensive acknowledgement to the International Civil Aviation Organization. The structure and accuracy of this thesis would not have been possible without the assistance of ICAO. I would like to first thank Mr. Mohamed Elamiri for permitting me to work within the Organization and making me a member of his team. I would like to thank Mr. Jitu Thaker, Mr. Mauricio Siciliano, Mrs. Cornelia Fisher and Mr. Alfonso Fonseca and for their valuable input towards my paper.

I would also like to thank personally Dr. Ruwantissa Abeyratne and Dr. Ludwig Weber for their continuous support in the furthering of my thesis. Dr. Abeyratne and Dr. Weber have also believed in my capacities and have permitted me to fulfill the goals that I have set for the furthering of my career.

I would personally like to extend my deepest gratitude to Ms. Mary K. McMunn for all her assistance, knowledge, support throughout the conceptualization of my thesis. Ms. McMunn, Chief of Facilitation, has guided me into being able to accurately describe the objectives I should set for my thesis. She has also given the opportunity to demonstrate my capabilities in the Facilitation field.

Finally, I would like to send my gratitude to Mrs. Maria D'Amico, Ms. Helen Manentis, Ms. Valerie Smith, Mrs. Jane Nounou, Mrs. Janice Ferguson, Mrs. Susie Tetteh, Mrs. Angelika Fuchs, Ms. Marjo Mikkola, Mrs. Jutta Wandzylak and Mrs. Colleen Gélinas for all their technical help in the realization of my thesis.

INTRODUCTION

Clearing Customs and Immigration formalities have always seemed to be associated with the concept of long waits, lengthily interrogations by officers, searches and seizures which amounted to an unpleasant experience and a question that many passengers ask themselves: to declare or not to declare...that is the question! The International Civil Aviation Organization [hereinafter referred to as ICAO], a specialized UN agency on civil air transport has attempted since the beginning of its existence to facilitate the movement of passengers and cargo.

ICAO was created following the *Convention on International Civil Aviation* [1], which was the first legal tool implemented concerning the regulations of civil air transport. As this Convention has a binding effect for Contracting States that have ratified it, provisions pertaining to the promotion of passenger facilitation were the inspiration for Customs Authorities to develop a system of advance notification on the identity of passengers entering a State. Thus came the concept of Advance Passenger Information [hereinafter referred to as API] and Passenger Name Record [hereinafter referred to as PNR].

The purpose for API and PNR access is to enable border control authorities to process passengers quickly through a mechanism of sending data in advance to customs

[1] *Convention on International Civil Aviation*, 7 December 1944, UN Doc. 7300/6 (1980)**[Chicago Convention]**.

officials[2]. There are many legal aspects that can arise from the time the passenger's information is read to the moment when the Border Control Authorities receive this data. Legal issues concerning privacy rights and data access as well as data storage require attention or at the least some consideration. Although, for many years, States have signed Memorandums of Understanding with air carriers so that such information would be sent on a volunteer basis, new recent legislative changes have made States and air carriers become apprehensive as the information requested by these new changes are much more extensive and have a compulsory character to them. For example, since September 11th, 2001, the United States have adopted laws changing this voluntary practice into a condition to continue maintaining landing rights.

The purpose of this thesis is to do a legal analysis of API and PNR access. In order to accomplish such a task, this study will be divided into three chapters. The first chapter will present an explanation and historical overview of API and PNR referring to laws and guidelines that certain States have adopted following September 11th, 2001.

The second chapter of the thesis discusses Machine Readable Travel Documents [hereinafter referred to as: MRTD]. The study of MRTDs is necessary in order to understand the concept of API as it is the information gathered on the travel document once read in addition to the information manually keyed in at check-in that is sent as API

---

[2] Dr. Ruwantissa Abeyratne, "Intellectual Property Rights And Privacy Issues-The Aviation Experience In API And Biometric Identification" (2002) **5:4** J.W.I.P. 632.

to the different Border Control Authorities.[3] For example, when a traveler is booked on a flight, he or she must submit the machine readable travel document to the check-in agent prior to departure. Once the document is read and API data is collected, the information is sent to Border Control Authorities by an electronic messaging system which shall be further explained in chapter 1 of this thesis.

The second chapter also refers to biometric procedures. Biometrics can be defined as characteristics that are measurable on a physical basis. Its purpose is to either confirm the identity of the passenger that presents his MRTD or to serve as a identification tool.

At the present time, MRTD possesses one form of biometric identification: the facial image, a physical characteristic of the person. However, in the future, an IC chip containing one or more biometrics could be added to an MRTD in order to enhance security and make border control clearance become more efficient.[4]

The final chapter makes an in-depth analysis towards privacy rights that each individual has and if there are possible violations of these rights with access to API and PNR data.

---

[3] In this respect, The Association of Asia Pacific Airlines has written:

> And, for API, they can pass on machine-read information electronically to the destination country for preliminary data checks before the aircraft lands there, thus speeding up processing on arrival.

Association of Asia Pacific Airlines, "Passenger Facilitation-A New World Order-2002 Annual Report", online: Association of Asia Pacific Airlines < http://www.aapairlines.org/content/annualreport/API.pdf > (date accessed: 7 January 2003)

[4] With this respect, the WCO/IATA/ICAO has written:

> Machine Readable Travel Document (MRTDs) enhanced with biometric identification are key to accelerating the clearance of passengers at airports and tightening security[...] Biometrics provide the capability of accurately measuring biological features to confirm identity and represent a next generation addition to MRTDs.

WCO/IATA/ICAO, *Guidelines on Advance Passenger Information (API)*, WCO Annex I to Doc. PC0123E1 (2003).

Since the adoption of the *US Aviation and Transportation Security Act*[5], air carriers, foreign governments and IATA have expressed concerns regarding the transmission of API and especially concerning the access of PNR information. The concerns of sensitive data being the target of mishandling had resulted in the possible threat of the European Commission requesting the European Court of Justice to give an opinion on this matter.[6] However, on February 19th, 2003 the EU and the US Customs Service began discussing the privacy issue in order to find some resolutions respecting national privacy laws and at the same time complying with US laws.

The chapter on privacy issues will demonstrate the rights that a passenger has in regards to air transport. Furthermore, an analysis of both American and European court decisions will illustrate what is a breach of privacy, if there is an infringement of privacy and if so, is the infringement justifiable under the national security provision that is found under US legislation.

[5] U.S., H.R. Con., *Aviation and Transportation Security Act*, 107th Cong., 2001 **[Homeland Act]**.
[6] Unofficial interview of Francis Morgan of the European Commission (25 March 2003).

CHAPTER 1: ADVANCE PASSENGER INFORMATION (API) AND PASSENGER NAME RECORD (PNR)

1. ADVANCE PASSENGER INFORMATION (API)

1.1 Definition

One of the most accurate definitions of API can be found inside *Annex 9*[7] of the *Chicago Convention* at Recommended Practice 3.34:

"Where appropriate, Contracting States should introduce a system of advance passenger information which involves the capture of certain passport or visa details prior to departure, the transmission of the details by electronic means to their public authorities, and the analysis of such data for risk management purposes prior to arrival in order to expedite clearance [...]"[8]

Another definition can be found in the Draft Guidelines for API written in cooperation by the World Customs Organization (WCO), the International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO) in March of 2003:

"Advance Passenger Information (API) involves the capture of a passenger's biographic data and other flight details by the carrier prior to departure and the transmission of the details by electronic means to the Border Control Agencies in the destination country. API can also act as a decision making tool that border Control Agencies can employ before a passenger is permitted to board an aircraft. Once passengers are cleared for boarding, details are then sent to the Border Control Agencies for screening against their enforcement database(s) and can identify high risk passengers requiring for example more intensive questioning upon arrival [...]"[9]

The same guidelines also recommended that the following information concerning each individual passenger could be included as API data to be sent prior to border control clearance:

---

[7] *Annex 9 to the Convention on International Civil Aviation (Facilitation)*, 11th Ed. (Montreal: ICAO 2002).
[8] ***Ibid.*** at Recommended Practice 3.34.
[9] ***Supra*** note 4 at I/8.

- Official Travel Document Number;
- The Name of the State that issued this document;
- What is the type of official document;
- The expiration date of the travel document;
- Surname and given names of passenger;
- Nationality;
- Date of Birth;
- Gender;
- Other travel document used(including which type of document);
- Primary residence (country of primary residence and full address);
- Destination address (full address);
- Place of birth;
- Traveler Status;
- Place/port of original embarkation;
- Place/port of clearance;
- Place/port of onward foreign destination;
- Passenger Record Locator Number.[10]

ICAO had suggested that these requirements be the absolute maximum required for the air carriers to submit API.

[10] ***Ibid.*** at 18.

1.2 Legal Foundation for API

Advance Passenger Information find their fundamental legal roots within the *Chicago Convention* and its *Annex 9.*

1.2.1 Chicago Convention

The Convention was signed in Chicago in 1944 and created the International Civil Aviation Organization [hereinafter referred to as: ICAO]. The objectives of this Organization are set forth in Article 44 of the Convention, which include the more specific aspects of facilitation whilst ensuring a safe and orderly growth of international civil aviation throughout the world. This Convention creates means in order to ensure efficient air transport as well as promotes the safety and security of aviation operation.[11] Furthermore, States are given the right to ensure proper control in accordance with article

---

[11] The text of article 44 of the *Chicago Convention* reads as follows:

The aim and objectives of the Organization are to develop the principles and techniques of international air navigation and to foster the planning and development of international air transport so as to:

(a) Insure the safe and orderly growth of international civil aviation throughout the world;[...]
(c) Encourage the developments of airways, airports, and air navigation facilities for international civil aviation;
(d) Meet the needs of the peoples of the world for safe, regular, efficient and economical air transport;[...]
(h) Promote safety of flight in international air navigation;
(i) Promote generally the development of all aspects of international aeronautics.

See Chicago Convention, ***supra*** note 1.

13[12]. Each State can therefore exercise effective control on individuals crossing their border.

In accordance with ICAO's objectives, the modern traveler needs to be provided with rapid processing through the different stages of air transport, whether it implicates the air carrier's procedures or those set forth by the border control agencies. In article 22, the *Chicago Convention* recognizes the importance of facilitation with respect to each passenger:

"Each contracting State agrees to adopt all practicable measures, through the issuance of special regulations or otherwise, to facilitate and expedite navigation by aircraft between the territories of contracting States, and to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially the administration of the laws relating to immigration, quarantine, customs and clearance."[13]

With this in view, article 29 of the Chicago Convention already stipulated the legal obligation for all aircraft of States to collect some form of data regarding the carriage of passengers:

"Every aircraft of a contracting State, engaged in international navigation, shall carry the following documents in conformity with the conditions prescribed in this Convention:
[...](f) If it carries passengers, a list of their names and places of embarkation and destination;
[...]"[14]

---

[12] The text of article 13 of the *Chicago Convention* reads as follows:

> The laws and regulations of a contracting State as to the admission to or departure of its territory of passengers, crew or cargo of aircraft, such as regulations relating to entry, clearance, immigration, passports, customs, and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State.

See Chicago Convention, ***supra*** note 1

[13] ***Ibid.*** at art. 22.

[14] ***Ibid.*** at art. 29.

1.2.2 Annex 9

Standards and Recommended Practices (SARPS) were implemented to follow the Chicago Convention into *Annex 9* to the Convention, pertaining to facilitation issues. First adopted by the Council on March 25th, 1949, *Annex 9* was implemented in order to follow the guidelines set forth in article 37j) of the *Chicago Convention*. This particular article called for the international community to adopt SARPS dealing with customs and immigration procedures.[15]

Within *Annex 9*, as previously cited, there is a Recommended Practice inviting Contracting States to introduce a system of advance passenger information in order for authorities analyze such data and perform risk management of passengers prior to arrival in order to expedite clearance.[16]

1.3 History of Annex 9 SARPS

In 1948, ICAO's Facilitation Division introduced the need to reduce issuance of entry and exit visas. During this FAL Division, the council adopted recommendations that States had suggested in order to reduce the preparation time and inconvenience to the

[15] *See Annex 9*, ***supra*** note 7.

[16] ***Supra*** note 8.

traveler.[17] These issues were addressed in order to permit expeditious entry to and exit from States.

1.3.1 Origin of API Recommended Practice

The concept of API was discussed during the Tenth Session of the Facilitation Division in Montreal in 1988. It suggested a recommendation[18] that was only introduced during the Eleventh Session, which gave background information on API and comments from

---

[17] The text of Recommended Practices 8.1 and 8.4 of the 2nd Session of the FAL Division reads as follows:

> 8.1 (RP) In order to facilitate the unilateral and bilateral elimination of entrance visas for non-immigrants, but at the same time to provide a simplified form of control with respect to the movement of non-immigrants where such control is deemed necessary, the following uniform system should be adopted[...] 8.4 (RP) Each State should abolish exit visas, and reduce any other emergency exit formalities to an absolute minimum.

ICAO Secretariat, *Final Report Of The Second Session of the Facilitation Division*, 1948, ICAO Doc 5464-FAL, 535.

[18] The text of Recommended Practice B-11 reads as follows:

> "IT IS RECOMMENDED THAT
> a) Contracting States, where possible, undertake projects to examine the effects of various advance passenger information programmes (including as appropriate various manual and electronic collection and transmission methods) in facilitating the clearance of arriving passengers through the inspection processes at major international airports;
> b) Where data are transmitted by Electronic Data Interchange, procedures should conform to international message standards and formats;
> c) ICAO would undertake a study of Contracting States' experiences from the projects undertaken under a) above in the advance passenger information privacy issues and the facilitation and other benefits and costs, by types of programmes, for passengers, air carriers and Contracting States; ICAO should liaise with the Customs Co-operation Council and other appropriate international bodies to ensure proper co-ordination in this area, and to safeguard the interests of immigration authorities;
> d) ICAO would keep Contracting States fully informed of developments; and
> e) ICAO would, no later than 1992, report on the study to the Council, which would decide whether the findings and recommendations should be recommended to Contracting States

ICAO Secretariat, *Report of The Tenth Session of the Facilitation Division*, 1988, ICAO Doc 9527-FAL/10, 54.

Member States. The recommendation on the format of API was included in the 10th edition of Annex 9.[19]

The report of the Division session mentioned that the Members of ICAO were concerned about privacy issues that could arise from the usage of electronic information provided by the API system.[20]It is also noted in this report that any electronic messaging should be processed under the Electronic Data Interchange EDIFACT format [hereinafter referred to as: E.D.I., the Electronic Data Interchange for administrative Commerce and Transport], and become international practice, in order to create standardization between Contracting States. This process relating to EDI has already been acknowledged as a practical means of exchanging API data by ICAO.

---

[19] The text of the Informal Meeting with ACI on API reads as follows:

> 2.1 Article 29 of the Chicago Convention requires every aircraft engaged in international navigation to carry certain documents, including, for passengers, "a list of their names and places of embarkation and destination". Annex 9 specifies, in Standard 2.7, the presentation of a passenger manifest document shall not normally be required, and notes that if the information is required it should be limited to the data elements included in the prescribed format, i.e. names, places of embarkation and destination, and flight details.
> 2.2 It should be noted that the opinion of this Standard contemplated the passenger manifest as a paper document, which would have to be typed or written and delivered by hand. [...] It is widely recognized that in any system involving the exchange of information (automated or not), it is the collection of data, which is the major expense. Increases in data collection requirements should result in benefits that exceed the additional costs. This principle was a central issue during the debate over API in the Tenth Session of the Facilitation Division (FAL/10) and the eventual adoption by FAL/11 of API systems as a Recommended Practice.

ICAO Secretariat, *Informal Facilitation Area Meeting in Consultation with ACI on Advance Passenger Information*, 1997, ICAO Doc INF/FAL/DJE WP/11

[20]The text of the Tenth Session of the Facilitation Division reads as follows:

> There was, however, considerable support for both B-type Recommendations although several delegates pointed out that there would be a need for the programmes concerned to take into account the importance of the privacy of the individuals reflected in the data protection laws already adopted in many States.

See ***supra*** note 18 at 53.

1.3.2 World Customs Organization

During The Eleventh Facilitation Division Session[21], suggested a recommended practice[22] where Contracting States should introduce a system of API as per the common guidelines of the World Customs Organization.[23].

---

[21] ICAO Secretariat, *Report of the Eleventh Session of the Facilitation Division,* 1995, ICAO Doc 9649 FAL/11.

[22] The text of the Eleventh Session of the Facilitation Division at R.P. 3.14.2 reads as follows:

> 3.14.2 Recommended Practice.-Where appropriate, Contracting States should introduce a system of Advanced Passenger Information (API), which involves the capture of passport details prior to departure and the transmission of the details by electronic means to the authorities in the destination country, and in so doing so should follow the joint World Customs Organization(WCO/International Air Transport Association (IATA) Guideline on Advance Passenger Information, except that the data elements to be transmitted as set forth in the Guideline should also include the nationality of the passport holder expressed in the form of the Alpha-3 Codes specified in ICAO Doc 9303. To avoid extra handling time during check-in, the use of document reading devices to capture the information in machine readable documents should be encouraged.

See ***Ibid.*** at 27.

[23] *See* the World Customs Organization, online: < www.wcoomd.org> (date accessed: 10th December 2002). The WCO was set up in 1847 from all thirteen European Government wanting more inter-Trade [hereinafter referred to as: GATT]. In 1948, two sub-committees were formed and a Convention on customs expertise and policies came in force in 1952 establishing the Customs Co-operation Council [hereinafter referred to as :CCC] which is headquartered in Brussels. In 1994, this Council became the WCO as working name. The text of its main mission is as follows:

> -Establishes, maintains, supports and promotes international instruments for the harmonization and uniform application of simplified and effective Customs systems and procedures governing the movement of commodities, people and conveyances across Customs frontiers;
> -Reinforces Members' efforts to secure compliance with their legislation, by endeavoring to maximize the level of effectiveness of Members' co-operation with each other and with international organizations in order to combat Customs and other transnational offences;
> - Assists Members in their efforts to meet the challenges of the modern business environment and adapt to changing circumstances, by promoting communications and co-operation among Members and with other international organizations, and by fostering integrity, human resource development, transparency, improvements in the management and working methods of Customs administrations and the sharing of best practices.

This was later implemented in the 10th Edition of *Annex 9* and consequently modified during the 11th Edition adding among other aspects the concept of risk management.[24]

One of the WCO mission, through the Permanent Technical Committee, was to develop a convention in order to modernize the changing structure of international trade and the evolution of Customs techniques and therefore facilitate States adopting national legislation. In 1973, the Council of the WCO adopted in Kyoto the *Convention on The Simplification and Harmonization of Customs Procedures*, a.k.a. The Kyoto Convention.[25]

The WCO's main objective is to simplify border control formalities and create effective border control for the rapid clearance of passengers. This objective is stipulated in its recommended practice in the *Kyoto Convention* as well as in the associated benefit provision[26]:

---

[24] The text of the Recommended Practice 3.34 of Annex 9 reads as follows:

> Where appropriate Contracting States should introduce a system of advance passenger information which involves the capture of certain passport or visa details prior to departure, the transmission of the details by electronic means to their public authorities, and the analysis of such data for risk management purposes prior to arrival in order to expedite clearance. To minimize handling time during check-in, document reading devices should be used to capture the information in machine readable travel documents. When specifying the identifying information on passengers to be transmitted, Contracting States should only require information that is found in the machine readable zones of passports and visas that comply with the specifications contained in Doc 9303 (series), Machine Readable Travel Documents. All information required should conform to specifications for UN/EDIFACT PAXLST message formats.

See ***supra*** note 7

[25] *Convention On the Simplification And Harmonization Of Customs Procedures*, online:<http://www.unece.org/trade/kyoto/ky-01-e1.htm#Historica> (date accessed : 3 January 2003)**[Kyoto Convention]**.

[26] The text of the *Kyoto Convention* at article 5 of Annex J reads as follows:

> Recommended Practice 8 : The Customs, in co-operation with other agencies and the trade, should seek to use internationally standardized advance passenger information, where available, in order to facilitate the Customs control of travelers and the clearance of goods carried by them.

"The benefit to Customs is the receipt, in advance of the arrivals of travelers, of information that will aid risk management with the objective of more precise targeting of Customs control. A benefit to travelers is that, on the basis of Customs analysis and evaluation of API, their risk status can be determined prior to arrival in the country concerned. Greater precisions in Customs targeting should result in the vast majority of travelers being assessed as presenting negligible or no risk and thus subject to minimal or no Customs control on their arrival."[27]

It is also noted that as a whole, the Convention is generally aimed at developing a system of pre-clearance to utilize waiting time prior to the departure of an aircraft in order to carry out formalities, which might otherwise delay passengers upon arrival of that aircraft at destination.

1.4 Advance Passenger Information Guidelines

The use of API became more and more a priority during the 1993/1994/1995 triennium and IATA acknowledged in a greater capacity the necessity for API implementation.[28]

In 1993, IATA and the WCO formally introduced the formal WCO/IATA guidelines following a Working Paper presented by the ICAO Secretariat during the Eleventh Session.[29]

Ibid.

[27] ***Ibid.***

[28] ICAO Secretariat, *Working Paper on Advance Passenger Information Further Development of ICAO Doctrine*, 2002, ICAO Doc FALP/4-WP/2.

[29] The text of the Eleventh Session of the Facilitation Division at Paragraph 4.2.4 reads as follows:

> 4.2.4 Furthermore, given the practical and cost constraints of data capture and transmission, limiting the required information to that which can be captured by machine reading passports and visas, augmented by basic flight details, is a prerequisite. To this end, IATA sees particular benefit in co-operating with the CCC to define the data and message sets for API within the UN/EDIFACT PAXLST development, and in establishing jointly agreed principles which can expand the benefits of automating and integrating all elements of the passenger process from origin to destination."

In the preamble of the guideline[30], it is indicated that because of the increase of passenger traffic, Customs are strained to process much more additional data when a traveler clears border control. Furthermore, in order to prevent increase in delays, the need for efficient automated processing has become a necessity, an issue that has been also supported by IATA.[31] According tot he WCO, API should also be considered uniform electronic text capturing by the UN/Edifact PAXLST Messaging system: "API permits a very thorough and rigorous screening of inbound passengers to be carried out, targeting those that

---

See ***supra*** note 21 at R.P. 4.2.4.

[30] The Customs Co-operation Council recommended standardization for API interoperability and an objective to control costs to airlines The text of the Eleventh Session Facilitation Division at R.P. 4 reads as follows:

> [...] requests Members of the United Nations Organization or its specialized agencies, and Customs or Economic Union which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions which have accepted this Recommendation.

Ibid. at R.P. 4.

[31] The text of the Eleventh Session Facilitation Division at R.P. 5 reads as follows:

> IATA has constantly sought to eliminate unnecessary forms and procedures in international air transport and the abolition of the passenger manifest has been an important policy objective for the Association. Recent opportunities to automate government control processes have, however, let to a close look at the concept of API and its potential for facilitation improvements.
>
> Collection of passenger details at departure presents a problem of additional workload for airlines t point in the system where staff and facilities are frequently already stretched to maximum capacity and beyond. Consequently, carrier support of API depends heavily on there being truly realizable benefits for airline passengers on arrival at destination.
>
> Furthermore, given the practical cost constraints of data capture and transmission, limiting the required information to that which can be captured by machine reading passports and visas, augmented by basic flight details, is a prerequisite. To this end , IATA sees particular benefit in co-operating with the CCC to define the data and message sets for API within UN/EDIFACT PAXLST development, and in establishing jointly agreed principles which can expand the benefits of automating and integrating all elements of the passenger process from origin to destination.

Ibid. at R.P. 5.

present the highest risk and allowing for the faster throughput of low risk travelers".[32] IATA also notes the necessity to create a limitation of how much data should be sent in order to address the concerns it had regarding costs as well as the potential for errors regarding the transfer of data. It suggested that information pertaining to the flight should consist of:

- Flight Identification;
- Scheduled departure date;
- Last place/port of call of aircraft;
- Place/port of aircraft initial arrival.

During the Eleventh Session of the Facilitation Division held in Montreal in 1995, the position of the WCO, formerly CCC, Customs Cooperation Council, in 1992, wrote guidelines for API mainly promoting the following aspects:

" - *Information Technology*
- *Greater co-operation between Border Control Agencies domestically;*
- *Greater international co-operation between Customs administrations and with other Border Control Agencies;*
- *Greater co-operation between Border Control Agencies and carriers.* "[33]

This was achieved by a recommended practice of the CCC:

"4.1.4[...] (a) Providing its Members with information on the technique of API benefits it can bring;

---

[32] ***Ibid.*** at R.P. 9.

[33] ICAO Secretariat, *Eleventh Session Information Paper On Advance Passenger Information (API) Guidelines Adopted by the WCO*, 1995, ICAO Doc FAL/11-IP/2 at point 3.

(b) Providing a forum in which the constraints on API can be discussed and hopefully resolved; and
(c) Seeking to jointly agreed standards with the airline industry so that API does not develop and proliferate in an inconsistent or unstructured way."[34]

In April of 2002, during a Facilitation Panel in Montreal on API, it was recommended to adopt additional provisions in order to fulfill the WCO's objectives:

- The usage of API for immigration, quarantine and aviation security (AVSEC) applications to customs;
- The internet or other PC-based systems and wireless technologies should be considered for the exchange of data rather than specify UN/EDIFACT syntax for data interchange;
- API should be part of a total border management system, machine readable passports with electronic visas, automated entry/exit records instead of embarkation or disembarkation cards and as well as interoperability of API systems with other States;
- Applicable Standards and Recommended Practices (SARPs) should leave the possibility of including biometrics into Recommended Practice 3.34 of Annex 9 (11th Edition);
- ICAO should measure the programme's success in operational efficiency and reduction of airport congestion.[35]

[34] ***Ibid.*** at point 1.3.
[35] ***Ibid*** at point 4.1.4.

In general, the WCO regards the receipt of API data as being a viable solution for border control clearance. To continue in this work frame, the WCO also announced in its recommendation, as a precautionary measure, that information be kept to a strict minimum. Otherwise, air carriers would be faced with the additional burden of assuming additional time and costs:

"Perhaps the most critical aspect of API is the means by which the data to be transmitted to the Border Control Agencies in the destination country is captured. Data capture can be costly, time consuming, labor intensive and error prone. The capture of data concerning departing passengers at the airport of departure introduces a delay in the check in process that could, if not managed properly, offset the potential advantage to passengers provided by efficient API applications. If the check-in process in unduly prolonged, then API will simply shift much of the delays and congestion away from the arrival area to the departure area. It is vital therefore that the effect of API on the check-in process is kept to the absolute minimum."[36]

The WCO also claims that API can also reduce staff costs because of this automated process that can therefore bring some form of saving for the air carrier.[37]The US Customs Service described within the WCO Guidelines a limitation to this process: API information should be sent to the US as APIS only if the flight originates or departs from the US.[38]

---

[36] ***Ibid.*** at clause 8.2.1.

[37] ***Ibid.*** at clause 6.9.3. And 6.3.

[38] The text of the US Customs Service within the WCO Guidelines at clause 3 and 4 of Attachment A reads as follows:

> (3) A general request to oblige the carrier to give access only to passenger name record information relating to passengers whose itineraries include at least one flight operated to or from or within the United States. In the event that carrier's systems are not designed or configured so as to allow such access without also giving access to information about other passengers, the Customs Service shall adopt procedures or take other appropriate measures to ensure that its officers do not access information relating to such other passengers. In addition, prior to implementing any online processes, the Customs Service will agree to appropriate security protocols with the carrier.
>
> (4) No carrier shall be obliged to change or modify its computer systems (hardware or software) in order to comply with a general or specific request, unless the changes or modifications and the allocation of the cost of making them are agreed in advance between the carrier and the Customs Service.

See ***supra*** note 4 at clause 3 and 4.

2. PASSENGER NAME RECORD (PNR)

Passenger Name Record Information is closely linked with API information as it is currently an information tool that could give additional information to Customs Officials. It does however substantially differ to API as it is a business document belonging to air carriers that may be accessed by customs officials. PNR is therefore not a governmental creation, but rather a business tool belonging to private entities, the air carriers, in which the possible usage raise sensitive issues.

The best definition that can be found is within the United States Passenger Name Record Final Rule:

"Passenger Name Record information that air carriers would need to make available upon request under section 44909 (c)(3) and section 122.49b refers to reservation information contained in an air carrier's electronic reservation system and/or departure control system that sets forth the identity and travel plans of each passenger or group of passengers included under the same reservation record number with respect to any passenger flight in foreign air transportation to or from the United States."[39]

The US Final Rule also stipulates the essential elements that may be accessed by customs officials:

- Name of passenger, date of birth, address and phone number;
- Passenger name record locator number;
- Travel agency name
- Ticket information;
- Form of payment for ticket;
- Itinerary information with carrier information;
- Seating and other PNR history on file.

According to the WCO, the Passenger Name record can be identified similarly to the US Final Rule: the entire air carrier booking including flight segments, seating arrangements,

[39] *Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States of 2001*, 66 Fed. Reg. 67482 (2002).

meal preference, medical condition of passenger and all other data that is stored this reservation file.[40]

Although the WCO gave a definition of PNR, many entities, such as travel agencies and air carriers are not aware of the actual PNR requirements that are evaluated and are under the impression that greater elements are examined by custom officials, such as meal preference and medical condition[41]. It is therefore important for governmental agencies and airlines to understand what kind of PNR information may be accessed and also to what extent this is done.

3. CONTRACTING STATES APPLICATION OF API AND PNR ACCESS

3.1 The United States of America

Due to the events of 2001, President George Bush signed the *US Aviation and Transportation Security Act* on November 25th 2002 making mandatory API transmission and PNR access to all passengers arriving in the United States. The Department of Homeland Security will therefore ensure that the air carriers, travelers and other governmental agencies comply with this new bill.

The US's Bureau of Customs and Border Protection developed a system of information called *Advance Passenger Information System* (hereinafter referred to as: APIS). This

[40] ***Supra*** note 4.
[41] Report from a UK based travel agency [unpublished].

system consists of data being collected by the air carrier and confirmed once the passenger's MRTD is read. Then, this data is formatted into the airline's reservation system. This information is then initially screened through Interagency Border Control Systems, a centralized database, which once processed is sent to the port of arrival into the United States.

The purpose of APIS is to accelerate the processing of inbound passengers and potentially give advance notice to these customs officials of high-risk individuals that would require additional questioning by Customs Officers. According to the WCO/IATA guideline[42], API transmissions should originate from the last port of departure from overseas before entering into the first port of arrival in the destination country.

In conformity with this Security Act, air carriers must submit API data to the US. In response to this legislation, Canada reached agreements with the US regarding APIS. According to the US Customs Service, a *Canada Smart Border/30 Point Action Plan*, better known as the *Manley Ridge Agreement* was implemented in December 2001 where the United States and Canada agreed to share API and passenger name records as of

---

[42] The text of the WCO Guidelines at clause 8.1.5 reads as follows:

> It should be noted that API transmissions will contain data for passengers carried into a country (initial place/port of arrival) from the last place/port of call of that aircraft abroad. API transmissions will not provide information of passengers previous flights or ports of call before joining the flight at the last foreign port of call. Neither will API transmissions provide information on onward flights to other countries. Put simply, the API transmission contains only details of passengers carried from last port of call to the first port of call in the country of arrival without regards for the passengers' initial point of departure or their ultimate destination.

Ibid. at clause 8.1.5.

spring 2003.[43] The Deputy Prime Minister of Canada, John Manley and the US Director of Homeland Security, Tom Ridge concurred of the necessity of reaching an understanding in order to promote national security.

The new *American Transportation & Security Act* stipulates in section 115 that the required information from each flight prior to departure and arrival in the United States should be as follows:

> " *A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:*
> *(a) The full name of each passenger and crew member;*
> *(b) The date of birth and citizenship of each passenger and crew member;*
> *(c) The sex of each passenger and crew member;*
> *(d) The passport number and country of issuance of each passenger and crew member if required for travel;*
> *(e) The United States visa number or resident alien card number of each passenger and crew member, as applicable;*
> *(f) Such other information as the under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety" (underlined by author of thesis [...]"*[44]

Furthermore, according to sub-section 4 of the same section on Passenger Manifests, the Customs service also can prescribe the time frame in which electronic messaging from air carriers as well as passengers name records and all pertinent identification necessary for screening can be received.

---

[43] The text of the *US-Canada Smart Border/30 Point Action Plan* reads as follows:

> The United States and Canada have agreed to share Advanced Passenger Information and Passenger Name Records (API/PNR) on high-risk travelers destined to either country. Canada implemented its Passenger Information system (PAXIS) at Canadian airports on October 8, 2002 to collect Advance Passenger Information.. The automated US-Canada API/PNR data-sharing program will be in place by spring 2003

US-Canada Smart Border/30 Point Action Plan, online : <http://wwww.whitehouse.gov/news/2002/12/20021206-1.html > (date accessed : 17 December 2002).

[44] ***Supra*** note 5 at section 115 sub-section 2.

Sub-section 3 gives the right to Customs Service to access the PNR file according to the number provided within the APIS transmission. This particular paragraph has spurred a great deal of controversy within Member States and air carriers having to comply with this Final Rule. It is important to stipulate that Customs Service do not routinely access PNR, nor d are to access such PNR information upon request and is done on a case by case level.

In response to this occasional PNR request access, the European Commission expressed concerns regarding national privacy legislation that would prevent the access to PNR information. Mainly, the EC was concerned that the data contained within the PNR would be used for commercial purposes and disclosed to an unlimited amount of agencies:

"In the EU there are serious concerns about personal data protection in this context, notably regarding inter alia the treatment, length of storage and scope of the data collected, access by third parties, and access to redness. These concerns are shared by the European Commission, the Data Protection Authorities (DPAs) in the EU Member States, and Members of the European Parliament. Some citizens have already submitted complaints to their DPAs, and there has been a reasonable amount of coverage of the issue in the media."[45]

The European Union also founded their concerns on the *European Directive* (95/46EC) as this directive prohibits any disclosure of private data. It further introduced seven principles as conditions of compliance with new US legislation, otherwise referred to as *Safe Harbour Principles*:

[45] Letter from the Directorate-General for Energy and Transport of the EC to ICAO (18 June 2003).

"- *Notice must be given to individuals informing them of the purposes for which their data has been collected and how it will be used;*
- *Choice must be offered to individuals, allowing them to choose (opt out) whether and how their personal information is disclosed to third parties or used for purposes which differ from the ones which were originally notified;*
- *Onward transfer of personal data by organizations to third parties must be consistent with the principles of notice and choice;*
- *Security of personal data must be maintained using reasonable precautions;*
- *Data integrity must be ensured so that personal data is relevant for the purposes for which it used, not processed in ways which are incompatible with the purposes for which it has been collected and steps taken to ensure that it remains accurate;*
- *Access to personal data must be maintained so that individuals can ensure that it is corrected or deleted where inaccurate;*
- *Enforcement should be available through independent recourse mechanisms to deal with complaints, disputes and remedies, and provide sufficiently rigorous sanctions to ensure compliance."*[46]

Although these principles were drafted, the EU also raised their concerns to the Secretariat of ICAO in June of 2003. It is also important to indicate that the EU has been attempting since February 2003 to resolve national data privacy legislation by the drafting of an agreement. In this agreement, US Customs Service agreed to address the EU's concerns by:

- Respecting the *Freedom of Information Act*[47] (hereinafter referred to as FOIA) that would limit the disclosure of data that is accessed when a clearly unwarranted infringement of personal privacy is committed. Furthermore, according to the FOIA, should this information be for law enforcement purposes, it will not be disclosed;

-Take extraordinary measures in the training of its employees conducting such PNR access;

[46] Joint Statement of the European Commission/ US Customs Talks on PNR Transmission (17-18 February 2003).
[47] *Freedom of Information Act*, 5 U.S.C. § 552 (1996).

-Non-transmission of any PNR information to any foreign, federal, state or local agency, unless for law enforcement purposes, national security may deem it necessary to do so. [48]

Should such agreement become force of law, it would have a binding effect between EC States and US Customs. Furthermore, it would not infringe on any national privacy legislation.

3.1.1 Air Carrier's Comments towards APIS and PNR Access

As a response to this new API data transmission and PNR access, American carriers such as American Airlines and Continental Airlines have agreed to comply with the new legislation but have requested the US Customs Service to review its penalty procedures should APIS data be incorrectly transmitted or not accomplished in a timely fashion.[49]

As for the Canadian air carriers, concerns were expressed in regards to the obligations relating to APIS. For example, a leading charter Montreal based airline, Air Transat (A.T.) requested from the US Customs a delay until December 15th, 2003 in order to fully comply with the new Interim Rule.[50] The airline's representative in government affairs indicated that the airline does not possess at this time any central reservation system as

---

[48] ***Supra*** note 45.
[49] Letter from American Airlines to US Customs (28 February 2002). Unofficial letter from Continental Airlines to US Customs (28 February 2002).
[50] Letter from Air Transat to US Customs (28 February 2002).

most of its bookings are done through tour operators and other travel agencies. The costs relating to changing to a fully electronic accessible system would represent an investment of 1.3 million dollars. He further criticized the deadlines imposed by the United States:

"We trust that such best efforts to date will be properly considered and that the Final Rule will not unduly penalize or burden smaller or less sophisticated air carriers such as Air Transat, in terms of passenger reservation and seat inventory management, with an unreasonably expeditious effective date."[51]

Its counterpart, Air Canada, has now given to the US Customs Service all API information containing the PNR number. Furthermore, both carriers have never opposed Canada's legislation requesting API./PNR data, which shall be later explained in this chapter.

As for the UK, British Airways (BA) agreed with the new American legislation pertaining to APIS and Passenger Name Record (PNR) access. In a letter dated early March 2002[52], BA informed the Office of Regulations and Rulings of the United States of its support for an API system since it had already complied by a Memorandum of Understanding [hereinafter referred to as: MOU] with the US Customs in 1998. This MOU consisted of voluntary release of passenger information to the US. In light of this new *Aviation and Transportation and Security Act*, BA believes that an automated version would enable a more efficient method for the collection of data. BA also

---

[51] ***Ibid.*** at page 4.
[52] Letter from British Airways to US Customs (1 March 2002).

considered possible PNR access by Customs officials to be beneficial as long as it is not disclosed for any other purpose than national security.

British Airways also considers API as the best method of transferring passenger information from the airline system to the government. It considered the automatic PNR release and ruled that it would not affect the *UK Data Protection Act*[53]. BA also added that as long as the US Customs Service assumed all costs for the development of a computerized system to access PNR data, it would comply with this legislation.[54]

The air carrier also expressed the desire to maintain APIS information within the WCO guideline's limitation previously mentioned as well as only access PNR information pertaining to passengers bound for the US. [55]

Virgin Atlantic, another British carrier, had expressed concerns over PNR transmission as some information relating to a passenger's file could be private and would contravene the *UK Data Protection Act.*[56] According to Virgin, it is now a requirement under the *UK Data Protection Act* that recording of personal data of passengers are not to be disclosed

---

[53] U.K., H.C.,"UK Data Protection Act", (1998), online: <http://www.hmso.gov.uk/acts/acts1998/80029--d.htm#28 > (date accessed: 3 July 2003).

[54] ***Supra*** note 51 at clause 6.5.1 and 6.5.2.

[55] In this respect, British Airways has written on the 26th of August to the US Customs:

> There appears to be nothing in the Interim Rule to protect the security and integrity of the carrier's systems. This is essential for British Airways to have confidence that cooperation will protect the integrity of its departure control systems and the legitimate rights and interests of its passengers. The Rule should provide such protection and British Airways respectfully requests the Customs Service agree to a security protocol prior to any direct systems access[...] British Airways requests that the agreements be finalized before access is activated.

Letter from British Airways to US Customs (26 August 2002).

[56] Letter from Virgin Atlantic Airways Ltd. To US Customs (30 August 2002).

outside the territory of the European Economic Area unless enough protection can be assured. In order to achieve this, the US Customs Service Agency would have to adopt the *Safe Harbour Principles*, set forth by the European Commission, under EU Directive (94/46/EC).[57] According to Virgin management, this directive only permits European companies to disclose information to any foreign State outside the community if reasonable protection of this information can be achieved.

Britannia, a UK charter counterpart, had mentioned to the American authorities that it was not able to comply with the interim rule on API and PNR requirements because it did not possess the necessary computerized reservation system.[58] Furthermore, in regards to APIS, it urged the US Customs Agency to waive applicability of data transmission on flights that are not bound for the US. It also suggested reducing the penalties imposed on air carriers if compliance cannot be performed on time. The time frame allotted to airlines in regards to changing their reservation systems is also an aspect that should be considered for API transmission.

Qantas Airways (QF), Australia's leading air carrier, had expressed a similar position to the one expressed by British Airways by requesting additional time to the US Customs Service Agency in order to comply with APIS and on the interim rule pertaining to PNR information. QF also stipulated that its national legislation may have additional restrictions in regards to some information being disclosed to other US Federal

[57] " Data Protection" *Frashfields Bruckhaus Deringer*, online: <http://www/freshfields.com/practice/ipit/publications/22367.pdf> (date accessed: 6 February 2003).
[58] Letter from Air 2000 Limited to US Customs (26 August 2002).

Agencies.[59] Qantas had therefore asked the authorities to sign an agreement in order to prevent the US Customs Service[60] from sending such data to an undetermined number of agencies.

In response to this legislation, Germany's leading air carrier, die Deutsche Lufthansa Aktiengesellschaft, had informed the US Customs Service of some national legislative impediments. It has now fully complied as of March 5th, 2003, by interim. According to the in-house legal counsel of Lufthansa, it appears that this law could be implemented throughout the year of 2003 should the European Commission find some solutions on a long-term basis with the US[61].

Unless clear resolutions can be found, violations of the Federal Data Protection Act can be of substantial financial and legal consequence.[62]

---

[59] Letter from Qantas Airways to US Customs (22 August 2002).

[60] In this respect, Qantas Airways on the 22nd of August has written:

> Prima facie, Qantas has not identified any incompatibility between USCS Passenger Name Record (PNR) requirements and Australia's national protection laws. However the statement in the CFR that "PNR information that is made available to Customs electronically may, upon request, be shared with other Federal Agencies", requires further clarification. Specifically, whether or not carriers will be notified when and with whom this information is being shared and how the integrity of the data will be maintained during this process.

Ibid.

[61] In this respect, the Deutsche Lufthansa on the 30th of August 2002 has written:

> Implementation by Lufthansa in the first quarter of 2003 appears feasible, provided that the present legal issues can be resolved.

Letter from the Deutsche Lufthansa Aktiengesellschaft to US Customs (30 August 2002).

[62] In this respect, the Deutsche Lufthansa on the 30th of August 2002 has written:

> Administrative offenses are applicable and punishable by fines up to Euros 250,000.00 to anyone who, whether intentionally or through negligence, collects or processes personal data which are not generally accessible without authorization (Section 43 BDSG); additionally, certain violations of this law can also carry criminal penalties of up to 2 years imprisonment and/or fines up to Euros 250,000.00 per offense (Section 44 BDSG).

Ibid, at page 2.

As for Swiss International, Switzerland's main air carrier, APIS did not cause any infringement to its national law on data protection. However the compulsory access to PNR could cause legal consequences to the carrier unless certain conditions are met:

"*The unlimited access by a third party in a foreign jurisdiction to the entire PNR data of a Swiss air carrier, without legal safeguards described above, turns out to cause major legal problems for the carrier concerned [...]*

However, provided that data can be restricted to PNR data on in-/-outbound US-flights, SWISS might be able to comply with national data protection laws when providing PNR access to US Customs. Compliance with Swiss and European Data Protection law could be achieved, if (a) the air carrier receives permission from the Swiss National Data Protection Officer and (b) obtains the required guarantees from the US authorities (see Point 2.2 above), eventually by applying the "Safe Harbour" principles. Furthermore (c), the air carrier would have to change its booking procedures by asking the passenger for additional data and an explicit consent to make this data available to U.S. Customs and other explicitly named U.S. authorities."[63]

Swiss International Air Lines had also raised an issue with the US where it recommended the creation of a filter system in order to protect a potential leakage of information to other authorities in the US.

Other airlines, such as VARIG, Delta, Continental and Pacific Asian airlines had as well expressed some concerns towards the new *Final Rule RIN 1515-A06 on Passenger Name Record Information Required For Passengers On Flights In Foreign Air Transportation To or From the United States*[64]. In fact, according to VARIG, Brazil's leading air carrier, PNR access could violate the Brazilian Constitution where unless express authorization is

[63] Letter from Swiss International Air Lines to US Customs (26 August 2002).
[64] *Passenger Name Record Information Required For Passengers On Flights In Foreign Air Transportation To Or From The United States*, 67 Fed. Reg. 42710 (2002).

given by the traveler or by other competent authority, it cannot comply with this new legislation.[65]

The International Air Transport Association, IATA, which represents 274 member airlines, has also noted that considerable discussions should continue to be held with the US Bureau of Customs and Border Protection in order to assure its carriers that privacy laws are being complied with. IATA had founded its remarks on the *EC Directive (95/46EC)*[66] which regulates the processing of personal data for all countries falling under the European Union. According to IATA, if the United States would adopt the Safe Harbour Principles in accordance with the EC Directive, there would be sufficient protection for other States and their air carriers to effectively comply without being held liable for data transmission. However, this compliance would be lawful only if all agencies of the US receiving such data would also adopt such principles. Furthermore, it suggested prior to the Final Rule on PNR to the US Customs Service:

- *"[...]- 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;*

---

[65] In this respect, Varig on the 18th of September 2002 has written:

> Due to Constitutional provision, information contained in air travel reservations, which is of a confidential nature, can only be disclosed upon written request by competent public authorities, by public administrative agencies, by an individual passenger—with proper identification—or by a legal representative duly authorized by the passenger.

Letter from Varig's legal counsel to US Customs (18 September 2002).

[66] EC, *EC Data Protection Directive (95/46EC), Protection of the individuals in relation to the processing of personal data*, (Brussels: EC,1995), online : < http://wwwdb.europarl.eu.int/oeil/oeil4.Res213 > (date accessed : 5 march 2003).

- *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."*[67]

Although IATA had expressed some difficulties with the new Transportation Act, the US Customs Service Agency adopted the Final Rules on APIS and PNR as they were previously drafted in conformity with article 13 of the Chicago Convention. This provision does permit each Contracting State to establish which formality it deems necessary for border control clearance within its territory.

According to the European Commission, international resolutions with the US regarding APIS and PNR access must be found and adopted in an international standard of practice with the help of ICAO:

"The US side took note of the Commission side's view that a multilateral agreement was necessary in the longer run, the Commission believing it to be entirely impractical for all airlines collecting and processing data in the EU to have to operate under multiple unilaterally imposed or bilaterally agreed requirements. In the Commission's view, the best framework for such an agreement would be ICAO."[68]

Furthermore, ICAO studied APIS as a whole, including the mitigation of fines when information would not be transmitted and concluded that it follows the guidelines set forth by the Chicago Convention relating to border control clearance.[69]

---

[67] Letter from IATA to US Customs (26 August, 2002).
[68] Letter from the EC Directorate-General for Energy and Transport to US Customs (19 February 2003).
[69] Unpublished ICAO Inter-Memorandum.

3.2 The Canadian Position

Canada's Customs and Revenue Agency (CCRA) together with Citizenship and Immigration Canada (CIC) has now implemented an API/PNR regulation where all aircraft incoming to Canada must send in advance this information. It uses both data that is sent in the following manner: API that is read through MRTD with the PNR number is delivered to authorities in the EDI electronic messaging format. CIC and CCRA's goal with this data is:

"The main goal of the API-PNR system is to provide the capability for CCRA and CIC officers to be forewarned of individuals inbound to Canada that may require review. Officers are to be provided with a mechanism to schedule automated analysis of passenger data upon the notification the flight has departed for Canada and to be informed of any possible hits on the individual within the existing enforcement data sources. The officer may then view the results of the analysis prior to the aircraft arrival. Every query and review of passenger data will be audited."[70]

3.2.1 Legal Foundation for Canada's API/PNR Request

The *Canadian Immigration and Refugee Act*[71] came into force in June 2002. The Act prescribes required documentations and obligations on air carriers in conjunction with Part 17 of the Regulations issued by Citizenship and Immigration Canada [hereinafter referred to as:CIC].

It is of interest that, in section 148 of the IRPA, air carriers are required not to carry any person that is not in possession of required documents of travel. In the event that such

[70] ***Supra*** note 4 at Appendix I p. 31.
[71] *Immigration And Refugee Protection Act*, L.c. 2001, c.27 **[IRPA]**.

obligations are not fulfilled, section 278 prescribes the different penalties, which will be imposed to the transportation companies.

Part 17 of the implemented regulations by the CIC, section 269 contains relevant advance passenger information legislation including:

"*269: Details data elements that will be required under the Canadian Advance Passenger Information programs, including;*

(a) Surname, first name and initial(s) of any middle names;
(b) *Date of birth;*
(c) *Country that issued a passport or travel document, the citizenship or nationality of the traveler;*
(d) *Gender;*
(e) *Passport number or, if a passport is not required, the number on the travel document that identifies them; and,*
(f) *Reservation record locator or file number.*

This part also provides for government access to airline reservation systems at 269(2), and seemingly indicates that the government shall have access to any record at any time following its creation."[72]

It is important to note that paragraph 2 of the same legislation includes a disposition where any electronic messaging follow the existing UN EDIFACT PAXLST format.

In terms of Canadian privacy legislation, there are 2 major Consolidated Statutes and Regulations such as the *Access to Information Act* and the *Privacy Act*. Under the *Access to Information Act*[73], article 19 subsection 2 prescribes that:

" (2) The head of a government institution may disclose any record requested under this Act that contains personal information if
(a) the individual to whom it relates consents to the disclosure;
(b) the information is publicly available; or
(c) the disclosure is in accordance with section 8 of the Privacy Act."[74]

---

[72] **Ibid.** at Part 17 section 269.

[73] *Access to Information Act*, R.S. 1985, c. A-1.

[74] ***Ibid.*** at article 19.

The general provision would therefore permit disclosure of personal information concerning an individual. Concerning the *Privacy Act*[75], article 8 would permit disclosure of personal information to other government institutions, should the interest of the public supercede those of the individual:

"8.(1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed [...]

(m) for any purpose where, in the opinion of the head of institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates."[76]

The Canadian government developed the API/PNR System according to the WCO guidelines in order to provide the Canadian Customs and Revenue Agency as well as the Citizenship and Immigration Canada advance information. This personal information would be used in order to track potentially high-risk individuals that would require additional review during border control clearance.

Canadian Courts have as well in the past permitted privacy infringements if the interest of the State was of greater importance than that of the infringement. In 1991, the Supreme Court of Canada applied a test, the *Wigmore Test*, in order to justify privacy infringements in the interest of the protection of the public:

---

[75] *Privacy Act*, R.S. 1985, c. P-21.

[76] ***Ibid.*** at article 8.

"The Wigmore Test as to whether or not a communications is privileged requires that: (1) communications must originate in a confidence that they will not be disclosed; (2) this element confidentially must be essential to the full and satisfactory maintenance of the relation between the parties; (3) the relation must be one which in the opinion of the community ought to be sedulously fostered; and (4) the injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation." [77]

In this particular case, disclosure was permitted in order to protect the public's interest. The disclosure of personal information, although being a possible violation of the right of privacy, cannot be considered of greater interest under Canadian law. The *Canadian Charter of Rights and Freedoms*[78], a legislative tool often used to remedy violations of human rights, does permit the State to uphold the law in order to protect the freedom of society: "The *Charter of Rights and Freedoms* guarantees the rights and freedoms set out in its subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[79] With these legal provisions, it is possible that CCRA and CIC could possibly find legal remedy against privacy infringements in order to protect national security.

However, according to the Privacy Commissioner of Canada, complying with the United States new interim rule would infringe fundamental privacy rights and could possibly be used for other purposes. It views this as a comparison to a "Big Brother" database.[80] However, it should be mentioned that when a passenger travels, he or she implicitly gives up a certain amount of privacy in order to receive clearance at different border control

---

[77] R. v. Gruenke, [1991] 3 S.C.R. 265.
[78] *Canadian Charter of Rights and Freedoms*, Constitution Act, 1982, c.1.

[79] ***Ibid.*** at article 1.
[80] George Radwanski, "Privacy Commissioner of Canada: News Release" (9 April 2003), online: < http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_2_e.as >(date accessed: 8 November 2002).

authorities by submitting information already contained in the passport. This will be further discussed in the third chapter of this thesis.

3.3 The United Kingdom Position

The *Draft Immigration (Leave to Enter Remain) Order 2000*[81] was first introduced by Mrs. Barbara Roche, Minister of State, Home Office. During this Parliamentary Standing Committee discussion, the Ministry suggested that API systems could have a dual positive impact: not only would API permit a rapid clearance process within an airport for the traveler, but it would permit officials to prevent individuals from travelling and being then denied access to the other State. Furthermore, according to Roche, this will in no way diminish the role of customs officers who will have the possibility of examining each passenger as well as their baggage and other belongings.[82] She also stated that the immigration officer could still, at any point of border control, monitor the passenger traffic and inspect the traveler.

---

[81] U.K., H.C., "House of Commons Standing Committee on Delegated Legislation Draft Immigration (Leave to Enter and Remain) Order", (2000), online: <http://www.hmso.gov.uk> (date accessed : 4 March 2003)

[82] The text of the Draft Immigration Leave to Enter and Remain Order reads as follows at page 3:

> The power to grant or refuse leave to enter before a person arrives in the UK has two benefits. Advance passenger information could pre-clear certain low-risk school groups and recognized reputable tour groups, thereby speeding their progress through immigration control and removing the need for detailed, individual examination on arrivals. Alternatively, we might send immigration officers overseas, with the agreement of the Government concerned, to address particular pressure points. It also allows us to take advantage of future technological developments such as biometrics. Such measures will benefit the traveling public, carriers and the immigration service.

Ibid. at page 3.

The UK, under this new legislation, has enabled many different enforcement agencies to collect an intelligence database of potential high-risk individuals and prevent their entry.[83] Furthermore, under the assurance of such agencies, both carriers and government agencies have determined that such API legislation would be applied through a very rigorous and fair process[84] and compliance to privacy rights would have to be effective.

According to the *UK Data Protection Act* of 1998[85], personal information should be protected and disclosure should be limited. The original *Draft Immigration* order followed the same guidelines as this act. However, API and PNR are also used in order to detect potentially high-risk individuals. This Act also permits the waiver of such privacy protection at its article 28. This provision does exempt all personal data protections if the information is sent for national security purposes:

> *"28.-(1) Personal data are exempt from any of the provisions of-*
> *(a) the data protection principles,*
> *(b) Parts II, III and V, and*
> *(c) Section 55,*
> *if the exemption from that provision is required for the purpose of safeguarding national security."*[86]

---

[83] The text of the UK Regulatory Impact Assessment at point 12 reads as follows:

> The measure will enable the police to build an intelligence picture which will allow them to target and track terrorists in a way that has become essential in the aftermath of September 11 and the subsequent ongoing campaign against the threat of global terrorism.

U.K., H.C.,"Regulatory Impact Assessment : Introduction to Extended Powers of Information Collection On Passenger and Goods, Schedule 7 to the Terrorism Act 2000 (Information) Order", (2002), online : <http://www.homeoffice.gov.uk/atoz/pax_and_goods.pdf > (date accessed: 8 November 2002).

[84] The text of the UK Regulatory Impact Assessment at point 39 reads as follows:

> We are confident that the enforcement agencies would apply the legislation fairly, proportionately and appropriately requesting the information and the police utilizing it. This approach has been confirmed by representatives of the police at meetings with the carriers.

Ibid. at point 39.

[85] ***Supra*** note 52.

[86] ***Ibid.*** at article 28

The *Terrorism Act* of 2000 was then amended in 2001 with the introduction of the *Anti-Terrorism, Crime and Security Act*[87]. This act imposes on air carriers the advance transmission of information of its passengers. At subsection 119 of this new act, the UK opted for this type of measure in order to safeguard national security. The UK and the EU are still to this date debating the possible infringements of privacy of this act and the obligation of data transmission to other EU States.[88]

3.4 Initiative of the Kingdom of Spain

On April 5th, 2003, the Kingdom of Spain published in the Official Journal of the European Union a proposed Directive on the communication of passenger data.[89] Its objectives suggested the prevention of illegal migration and the further implementation of anti-terrorism legislation:

"Article 1: Aim-
Member States shall take the necessary steps to establish an obligation for carriers to transmit to the authorities responsible for carrying out border checks:
(a) at the time of boarding, information concerning the people they are preparing to carry;
(b) information on foreign nationals carried by them to the territory of the Member States and who, on the date stipulated on the travel ticket, have not returned to their country of origin or have not continued their journey to a third country. This information musty be transmitted at the latest within forty-eight hours of the date stipulated for the return journey or for continuing the journey to a third country.

The information referred to above shall comprise the number of the passport or travel document used, nationality, first name and family name(s) and the date and place of birth."[90]

---

[87] U.K., H.C., "UK Anti-Terrorism, Crime and Security Act", (2001), online: <http://www.hmso.gov.uk/acts/acts2001/10024--n.htm#119 > (date accessed: 4 July 2003).
[88] Interview of Mr. Timothy Fenoulhet of the EC Commission's Energy and Transport Directorate (5 July 2003).
[89] EC, *Initiative of the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data*,[2003] O.J.L.82/23.
[90] ***Ibid.*** at article 1.

The other provisions of this directive also discuss sanctions to air carriers that would not comply with such API request.

Following the presentation of this directive, the European Union considered this directive to be contrary to the EC Directive 95/46/EC as it would violate fundamental privacy rights. However, the Spanish Government has to this date considered adopting this directive into its national legislation which would oblige all carriers to transfer API in advance when departing or arriving in the Kingdom of Spain.[91]

3.5 The Australian Position

The Australia Immigration and Customs have already implemented API systems in order to accelerate the process and enhance border control.[92] In order to exchange API, Australia implemented the Advance Passenger Processing, hereinafter referred to as APP. This system provides a rapid clearance by the participating carriers and Border Control Agencies. Under the APP System, during the check-in process, the MRTD is captured by the airline at check-in and in cooperation with the existing visa, the passenger is then cleared electronically. APP uses two separate processing databases. The first one registers the passenger's movement while simultaneously being checked against a computerized consolidated Customs/Police/Immigration alert list. This enables

---

[91] ***Supra*** note 87.
[92] Australian Delegate to ICAO, *Facilitation Panel Fourth Meeting Information Paper*, 2002, ICAO Doc FAL/4-IP/8.

authorities to be forewarned if an individual is required to be examined by a Customs Marshall.

Furthermore, prior to an inbound flight, APP identifies the individuals before luggage is boarded on the flight.[93] APP also accelerates the process for border control clearance: the traveler's passport is read at foreign check points and a magnetic card is then given if authorization to travel is granted with the individual's details enabling him or her to use the "Express Lane" upon arrival in Australia.[94]

The APP System works in cooperation with the Electronic Travel Authority (ETA), which is a communications network. When data is captured, it is sent through the ETA system that verifies the validity of the visa for those passengers who require such travel documents as well as the status of Australian passports.

In order to legalize the APP System, the government has also amended national legislation in order to permit capture of data of API and access to PNR without infringing privacy rights.

---

[93] ***Supra*** note 4 at Appendix I p. 28.

[94] The text of the WCO Guidelines at clauses 3.2.5 and 3.2.6 reads as follows :

> At check-in, the airline prints the passenger's bio data and flight number on a special Australian Incoming Passenger Card with the word "EXPRESS" indicated. The card also has a magnetic strip that is coded with an identifier to retrieve that data on arrival in Australia.
>
> On arrival in Australia, the passenger will be directed to the appropriate processing lanes by use of dynamic signage and Customs marshals who are on-hand. APP passengers using the Express lanes are expected to be cleared in about half the time of other passengers who are not APP.

Ibid. at clauses 3.2.5 and 3.2.6.

As some carriers have voluntarily participated to this plan, it now remains to the government to implement mandatory procedures for APP.[95] According to Australian Customs Service, APP gives a quantifiable reduction in undocumented travels and therefore reduces the possibility of being imposed fines by other Contracting States for allowing a passenger to travel without proper documentation.

3.6 The German and Swiss Positions

According to currently applicable privacy laws, certain data is protected by the *Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG)*[96] and requires special permission from each traveler before permitting access to API and PNR information by other States. According to German law, all data must be deleted from any banks of information after a certain amount of time. As for the Swiss Government, personal data is regulated by the *Data Protection Act (DSG)*[97], and all transmissions must be transferred in good faith and must be done in a secure manner.

As the API transmission is currently used for purpose of border control inspections, it could be suggested that this would not infringe on the current Swiss and German provisions concerning privacy.

---

[95] ***Ibid.***
[96] German Federal Ministry of Interior, *Bundesdatenschutz*, (December 1990), online: <http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm#absch1 > (date accessed: 17 January 2003).
[97] Switzerland, *Swiss Data Protection Act*, (19 June 1992), DSG SR 235.1.

3.7 The Mexican Approach

Mexico currently requests API information on passengers and crew on all international flights and intends to submit to the United States with a minimum of 95% accuracy all information in the UN-EDIFACT messaging format. Mexico also plans to fully request API information itself and penalize air carriers that are either late or not submitting at all such information. Similarly to the US, it does plan to request on a case by case passenger name record data. If it does randomly, the record locator reference number would be sufficient.[98]

Mexico has also signed an agreement with the United States, otherwise referred to as the *Smart Border 22 Point Agreement*[99], stipulating that on a voluntary basis, Mexico would exchange some information with the United States mutually in order to prevent illegal migration and detection of potentially high-risk passengers. According to the US Customs Service, there is presently an exchange of information on international flights bound for Mexico even though the port of arrival is not the Unites States. For example, at this time, a flight from Frankfurt to Mexico City non-stop may have to submit to the US API as well as access PNR information on its passengers prior to arrival in Mexico[100].

---

[98] Secretaria De Gobernacion, Instituto Nacional De Migracion, *Technical Specifications INM Fast-Track Confidential INM Presentation* (2002) [unpublished].
[99] "Smart Border 22 Point Agreement" *US White House* (21 March 2002), online: < http://www.whitehouse.gov/infocus/usmxborder/22points.html > (date accessed: 8 July 2003).
[100] Unofficial statement given by Dennis Benjamin, US Customs Service (December 2002).

The Instituto Nacional De Migracion has proposed an electronic database collecting information of passengers when making a reservation, and, together with IATA and the Simplifying Travel Procedures, it established a data processing system to be used for API transmission and PNR access.[101]

3.8 Republic of Korea

At this stage, Korea also requests API information for all flights that are inbound. API is collected by MRTD at check-in and is then sent to Korean Customs Intelligence System (KCS) prior to boarding of a flight. This alerts the authorities of the arrival of individuals that would require additional inspection. API, in Korea serves two purposes: it alerts KCS of individuals requiring more questioning and it reduces the time in which a passenger is processed at border control.[102]

4. CONCLUSION

Although many air carriers deem that potential liability could be foreseeable, it is to be noted that under the *Chicago Convention*, a State has the right to request information in

---

[101] ***Supra*** note 97.

[102] The text of the WCO Guidelines at Appendix I p. 30 reads as follows:

> With the introduction of the API system and other measures to facilitate passenger process, the overall time taken to complete the clearance process, from the time of disembarkation to the exit from the customs has been reduced to less than 30 minutes to more than legitimate (non-selected) 95 % of passenger.

Supra note 4 at Appendix I/30.

order to ensure border control clearance.[103] Therefore, as national policy, a member State has the right to enforce upon others their requirements for clearance into their territory.[104]

The main purpose for Advance Passenger Information systems is to facilitate the passenger in order to ensure rapid border clearance as well as detect in advance potential high-risk individuals. In fact, within the WCO/IATA/ICAO Guidelines of March 2003, ICAO suggested that API be considered a secure method of ensuring efficient border crossings:

4.3.4. Current projects in the facilitation programme aim at a straightened and more efficient system of border controls at airports, which would raise the level of general security and at the same time yield measurable improvements in facilitation for the vast majority of travellers. API is potentially a valuable tool which States may use to achieve these objectives. An API programme's success can be measured by the increase in operational efficiency and reduction in airport congestion which are achieved."[105]

The usage of advance passenger information can be considered as a facilitation tool, but also serves the purpose of ensuring aviation security. The Chicago Convention stipulates in Article 44 d) the necessity for safe and efficient air transport. ICAO has recognized the fact that security and facilitation must act as a joint venture :

---

[103] The text of article 13 of the *Chicago Convention* reads as follows:

> The laws and regulations of a contracting State as to the admission to or departure from its territory of passengers, crew or cargo of aircraft, such as the regulations relating to entry, clearance, immigration, passports, customs, and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State.

Supra note 1 at article 13.

[104]The text of article 1 of the *Chicago Convention* reads as follows:

> The contracting States recognize that every State has complete and exclusive sovereignty over the airspace above its territory.

Ibid. at article 1

[105] ***Supra*** note 4 at clause 4.3.4.

" A recent organizational change at ICAO, in which the administration of the security and facilitation programmes was merged, recognizes formally the importance of establishing a good balance between the need for effective aviation security and the need to facilitate air travel."[106]

[106] Mary K. McMunn, "Aviation Security And Facilitation Programmes Are Distinct But Closely Intertwined" ICAO Journal 51:9 (November 1996) 7.

CHAPTER 2: THE UNDERSTANDING OF MACHINE READABLE TRAVEL DOCUMENTS AND BIOMETRIC PROCEDURES.

1. MACHINE READABLE TRAVEL DOCUMENTS (MRTDs)

Machine Readable Travel Documents are an important aspect of API as it is through MRTDs that information requested by other States as Advance Passenger Information can be collected. As the WCO stipulates in its draft for API guidelines: "Machine Readable Travel Documents (MRTD) and Document Readers are an important component in API. The use of this technology for data capture at the airport of departure can greatly reduce delays."[107]

1.1 Definition

MRTD can be defined as:

" [...] *an official document issued by a State or organization which is used by the holder for international travel (e.g. passport, visa, official document of identity) and which contains mandatory visual (eye readable) data and a separate mandatory data summary in a format which is capable of being read by machine."*[108]

Once a passenger proceeds to check-in, the MRTD is read by a machine and together with the information in the existing reservation file or information added manually, API transmission can be sent.

---

[107] ***Supra*** note 4 at page 22.

[108] *Machine Readable Travel Documents*, ICAO Doc 9303 (2002) at II-2.

1.2 Historical Background of MRTDs

Machine readable travel documents were first established in 1968 by the Air Transport Committee of ICAO by recommendation of Doc 9303 that establishes all guidelines pertaining to machine readable travel documents. The Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTDs) is constantly modifying these guidelines in order to maintain an accurate reflection of current technologies.

ICAO's mandate regarding machine readable travel documents was also reiterated during the Fourth Meeting of the Facilitation Panel in Montreal in April of 2002.[109] During this Panel, standardization of travel documents, rationalization of border control systems and security issues were discussed.

The following are issues given during the 2002 Ministerial Conference to the Panel for objectives to be achieved for the 2003 year :

"*a) substantial upgrading of specifications for machine readable passports, visas and other official travel documents, including crew documentation;*
b) production of new technical guidance in areas such as identity confirmation with biometrics and security features of travel documents;
c) further development of modern customs and immigration control concepts employing information technology and risk management; and
d) updating of ICAO doctrine on controls on fraudulent documents and handling of inadmissible persons."[110]

---

[109] ICAO Secretariat, *Information Paper: Facilitation Programme Support For Aviation Security-Submitted During The High-Level, Ministerial Conference On Aviation Security*, 2002), ICAO Doc FALP/4-IP/3.
[110] ***Ibid.*** at page 1.

1.3 Legal Foundation for MRTDs

ICAO's mandate to standardize travel documents originates from the Chicago Convention:

" a) the requirements for persons travelling by air and aircraft crews to comply with immigration, customs and passport regulations (article 13)
b) the requirement for States to facilitate border clearance formalities and prevent unnecessary delays (article 22); and
c) the requirement for States to develop and adopt internationally standard procedures for immigration and customs clearance (article 37(j)).[111]*"*

as well as within Recommended Practice 3.5 of the Convention's Annex 9 :

"When issuing passports, visas or other identity documents accepted for travel purposes, contracting States should issue these machine readable form, as specified in Doc 9303 (series), Machine Readable Travel Documents."[112]

1.4 MRTD Objectives

MRTDs have come to standardize travel documents in regards to the content of information to be provided. This standardization must also be accompanied with security precautions that a Contracting State must take when issuing an MRTD. In order to meet both criterias, Doc 9303 contains the following specifications:

"*3.1 Forgery. Reliable security measures shall be incorporated to facilitate the visual detection of any alteration to the MRTD. Such security measures should, if possible, also facilitate the automated detection of alterations. "Forgery" is defined as the fraudulent alteration of any part of the MRTD.*

---

[111] ***Supra*** note 107
[112] ***Supra*** note 7 at R.P. 3.3.

3.2 Counterfeit. To facilitate the visual and/or automated detection of counterfeits, a combination of reliable security features shall be incorporated in the MRTD. "Counterfeit" is defined as the unauthorized reproduction of the MRTD by whatever means.
3.3 Imposters. Security features should be incorporated to facilitate the visual and/or automated detection of the fraudulent use of the MRTD by an imposter. "Imposter" is defined as someone representing himself or herself to be some other person.
3.4 Materials. Whenever possible, materials should be controlled varieties which cannot be easily acquired for other than official purposes. Where materials are not of a controlled variety, it is recommended that additional features be integrated with these materials. When different types of materials are integrated to form the MRTD or any part thereof (e.g. paper substrate with laminate), they shall be assembled in a manner to prevent reuse and reassembly following separation for purposes of fraudulent alteration."[113]

There are many advantages for a State to issue documents according to Doc 9303. For example, the possibility of carrying inspections in a quick and timely fashion: the document can be processed by machine reading with a minimal probability for breaches of security, mistakes or delays caused by manual keying of data. MRTD standards also follow Recommended Practice 3.31 of Annex 9 that suggests a time frame of 45 minutes per passenger for border control clearance.[114]

According to current objectives, the study of biometrics will undoubtedly be a topic for discussion during the next TAG/MRTD meetings to be held in 2003 during the month of May. Biometric procedures represent new technologies to add to the current MRTD templates for every travel document that is currently issued.[115] Many States are now actively participating in the research of biometric procedures as authorities believe it to

---

[113] ***Supra*** note 107 at article 3.1 to 3.4.
[114] The text of *Annex 9* at R.P. 3.31 reads as follows:

> Contracting States, in cooperation with operators and airport authorities, should establish as a goal the clearance within forty-five (45) minutes of disembarkation from the aircraft of all passengers requiring not more than the normal inspection, regardless of aircraft size and scheduled arrival time.

Supra note 7 at R.P. 3.31.
[115] ICAO Secretariat, *MRTDs Optimizing Security and Efficiency*, ICAO Circular (2002).

be the most foolproof method for confirmation of identity of document.[116] During the Biometrics 2002 Conference, ICAO and the International Organization for Standardization (ISO)'s mandate was re-established concerning work on biometrics:

"While this initiative was exclusively focused on confirming the person's identity as the rightful holder of the travel document to assist in facilitating the growing volumes of air travelers, it had the additional capacity to help identify persons who should be denied entry to a country, prevented from boarding an aircraft or possibly even detained."[117]

These new biometric ID features should be added to MRTDs as well as implemented to other documents where confirmation of identity is required.

In conclusion, MRTD's have been developed as part of ICAO's mandate and continue to evolve with new technologies such as biometrics in order to ensure efficient and secure means for border control clearance. As Mrs. Raimonda Admine noted in her report to the TAG/MRTD Regional Information Point: "Doc 9303 aids facilitation and increases security".[118]

2. BIOMETRIC PROCEDURES

The study of biometric procedures goes hand in hand with the concept of MRTDs as it can only facilitate the screening and processing of identity confirmation with the pre-existing machine readable travel documents technology. Biometrics can be defined as

---

[116] ***Ibid.***

[117] *Conference on 2002 Biometrics of ICAO and ISO* [unpublished].

[118] Statement of Mrs. Raimonda Admine [unpublished].

characteristics that are measurable on a physical basis such as fingerprints, retinal and iris features, as well as facial characteristics.[119] Biometrics can prove to be very useful within the civil air transport border control processing. In fact, at the current time, Amsterdam Schipol Airport uses the iris biometric technology for processing efficient border control clearance. Iris consists of the reading of the eye in order to validly identify the traveler's record.

2.1 Limitations

At present, biometrics procedure have been found to lack in accuracy and present many obstacles relating to labor and privacy issues mainly in the sense that it requests the installation of a large central database of personal information.[120] Although these situations are currently still not resolved: "[...] the United States is demanding that all visitors have some form of biometric identifier attached to their travel documents, setting a deadline as soon as October next year."[121]

The United States have as well incorporated in their legislation measures that authorize the testing of biometrics, which is at this time being conducted in San Francisco's International airport.[122]

---

[119] Dr. Ruwantissa Abeyratne, "Biometric Identification Of Airline Passengers", [2002] Tolley's Comm. L.1.
[120] Karen Dearne, "Immature Biometrics ID Systems Flawed", *International Biometric Group* (3 March 2003), online: < http://www.biometricgroup.com/in_the_news/australian_it.html > (date accessed: 8 July 2003)
[121] ***Ibid.***
[122] U.S., *Air Transportation Security Act*, 49 U.S.C.S § 44903 (2002).

2.2 Legal Foundation

ICAO has been mandated through its reflection on MRTDs to include biometrics in order to facilitate the clearance of passengers at border controls. The legal foundation can be found at Article 37 of the Chicago Convention:

"[...] To this end the International Civil Aviation Organization shall adopt and amend, as may be necessary, international standards and recommended practices and procedures dealing with: (j) Customs and immigration procedures;[...]"[123]

Through a working committee that involves the Federal Aviation Authority, the United States Customs Service and the Federal Bureau of Investigation created a study group on the different biometric technologies in order to enhance border control protection and simplify the process of confirming identity of traveler. This report was first introduced within the aviation security realm in order to provide an infusion of these new technologies. It can be applied into four purposes:

- Employee identification
- Airport surveillance and protection of public areas
- Verification of passenger identification
- Verification of aircrew identity.[124]

---

[123] ***Supra*** note 1 at article 37.
[124] "Aviation Security Working Group Steering Group Analysis", 2001, online : <http://www.biometricscatalog.org/asbwg/Files/ASBWG_Steering_Committee_Analysis1.pdf > (date accessed : 9 March 2003).

2.3 Type of Biometric Procedures

There are five major types of biometrics that will be demonstrated in the current section.

The first type of biometric procedure is the digital fingerprinting. In fact, it can be compared to the previous method of stamping each finger on ink and the reproduction of the print on paper. This biometric procedure can then be read on a template which is mainly used at this time for law enforcement agencies such as criminal investigations. It can also be used for fraud investigation, facilitation of air transport and computer access.[125]

The second method of biometrics is the hand geometry system. It involves the reading of the hand without fingerprinting. Sensors separate the hand and verification is done through a reader[126]. This practice was also common before September 11th, 2001 when INS introduced the INS Passenger Accelerated System Services (INSPASS). INSPASS used hand geometry for border clearance of frequent flying travelers, aircrew on duty, other diplomats and representatives of international organizations of countries that were part of the visa waiver program. On February 28th, 2003, INS introduced the Automated

[125] ***Ibid.*** at page24

[126] ***Ibid.***

Inspection Services, which incorporated INSPASS systems and by interim rule determined that low-risk passengers could now keep their status for up to two years.[127]

The third method refers to facial recognition. Through spatial geometry, it can store facial features of an individual. The only disadvantage of this biometric is that with different lighting and other environmental conditions, it has been proven not to be foolproof. In fact, it involves a high risk of duplication: "Physical characteristics may vary from chemical composition of body odour, facial features, thermal emissions [...] and vein measurements to walk-pattern and posture".[128]

According to IATA and the *Simplifying Travel* [hereinafter referred to as SPT][129], facial recognition is to be the most recognized method of identification when clearing border control.

Furthermore, the Airports Council International also favors this type of biometric. As Heitmeyer quotes the factors favoring facial recognition to MRTD's:

---

[127] INS, "INS Extends Enrollment Period", 2003, online: < http://www.immigration.gov/graphics/publicaffairs/newsrels/sentriextent.htm > (date accessed: 9 March 2003)

[128] ***Supra*** note 123 at page 3.

[129] Refer to the SPT Brochure 2002. The Simplifying Travel Group is a joint venture with IATA in order to develop new technologies in biometrics for the screening of passengers. In this respect, the SPT has written:

> The SPT Program is a joint initiative amongst a number of organizations, representing passengers, airlines, airports, control authorities, travel agents and broad government interests, to measurably improve the passenger experience and enable security enhancement by:
> - Implementing biometrics and other new technologies;
> - Sharing information amongst service providers;
> - Enabling controls and services to be effected more efficiently.

Brochure from SPT (2002) "*Simplifying Passenger Travel*"

- " - *The potential for using the portrait on the MRTD during the computerized authentication stage;*
- *The fact that facial recognition is non-intrusive and does not require the person to perform an overt, time-consuming act to allow details to be captured, nor require the person to touch something;*
- *The fact that facial image can be captured repeatedly (where required), even when the person is at distance."*[130]

The fourth procedure is the iris recognition, which involves the reading of the eye's iris and comparing it with the ones already stored in a main centralized database. As an example of its application, Schipol International Airport in Amsterdam has now fully implemented this method.

2.3.1 Schipol Airport Iris System

The program in itself is called *Privium* and it offers the possibility for Dutch travelers to possess a special chip within their travel document for quick passage at border controls. The Dutch Immigration Authorities have approved Privium as being a valid border crossing measure. It is accessible to citizens of the European Community as well as the U.K., Iceland and Switzerland

The Dutch Authorities suggested that stored data of the individual's profile would not infringe on the passenger's privacy rights. In fact, Privium's terms and conditions stipulate to all individuals adhering to this program the possibility of accessing their

[130] ***Ibid.***

personal file and requesting amendments of stored information. It therefore does not violate in any way the current Dutch legislation on data protection:

"7.1 Schipol collects the personal data that the Participant filed in on the application form, as well as data on the use of the Privium Card by the Participant. The statutory regulations as laid down in the Wet Bescherning Persoongegevens (Personal Data Protection Act) are complied with by Schipol.
7.2 In the Privium card, the card number, the template of the iris scan, the name, place of birth and date of birth of the Participant are incorporated [...].
7.7 Schipol will, except in cases where the law so requires [...] not provide the Participant's personal data to other persons or institutions outside Schipol Group without the Participant's consent [...].
7.8 The Participant can inspect his/her own personal data after having made a written request to that effect to Schipol [...]."[131]

It could be suggested from the terms and conditions set forth by this program that the data collection does have certain limitations. In fact, it also specifies the possibility for Schipol to face possible lawsuits should its employees conduct any gross negligence or willful intent. This could be the case if an employee of Privium would distribute such information concerning a traveler without consent or where the law on this matter varies.

The fifth and final procedure is the voice or speaker recognition that measures a person's voice. However, according to the Aviation Security Working Group on Biometrics, a group consulted by US Customs, it has proven to be unreliable in the sense that it is prone to errors because a person's voice can be changed or even copied, as it is highly behavioral and physical.

---

[131] Privium Program, "Terms and Conditions of Privium", 2003, online: <http://www.schiphol.nl/schiphol/content/content_C_c_l.jsp?CONTENT%3C%3Ecnt_id=226867&FOLDER%3C%3Efolder_id=379167&guidenr=00&guidemode=vac&entry=90&bmUID=1047138237310&submenu=/Assortments/Main/Primary/Schiphol/General/menus/menu90/Algemene_Voorwaarden > (date accessed : 9 March 2003).

The International Biometric Group concluded in its final report that fingerprinting and iris technology had proven to be accurate and impossible to duplicate in the preliminary testing:

"*New counterterrorism laws, including the USA Patriot Act and Enhanced Border Security and Visa Entry Reform Act, require authorities to use biometrics to detect immigration fraud. Biometric technologies, such as fingerprint readers and iris scanners, use parts of the body that cannot be altered to identify people.*"[132]

The different methods of biometrics must also be evaluated on the basis of using secure technologies. To quote Abeyratne: "The main threat to a foolproof identification of biometric data and matching would be the hardware used in the process, which would be vulnerable to code-cracking and information leaking by unauthorized persons."[133]

2.3.2 The Mexican Approach

The Instituto Nacional de Migracion (INM) has now introduced technical specifications for Fast Track processing during border control. This system is based on Recommended Practice 3.34 of Annex 9 regarding API information which is sent by air carriers to immigration authorities prior to arrival. The individuals that are admissible to this program are separated into three categories:

-Frequent flying passengers

---

[132] Michael Hardy "Group Issues Final Biometrics Report", (28 February 2003), online : Federal Computer Week < http://www.fcw.com/fcw/articles/2003/0224/web-bio-02-25-03.asp > (date accessed : 9 March 2003).

[133] ***Supra*** note 118 at page 2.

-Travelers or individuals of countries that have signed agreements with Mexico accepting this new Fast Track processing;

-Individuals that do not represent high-risk travelers and have shown good behavior.[134]

Although showing some similarities with the Iris system in the Netherlands's Amsterdam Schipol Airport, these individuals are given badges that contain personal data information for quick efficient border clearance. These badges do conform to ISO Standard 7816 as an acceptable travel document containing a personal identifier data chip with the individual's pre-printed Fast Track number, the name of the passenger and birth date, a photograph as well as the nationality and passport number. The INM specifies that this system does not replace the necessity for travel documents, which can be requested at any time by INM officials.

These badges permit border control clearance by:

-Recovery of identifier of passenger by biometric fingerprinting that is authenticated by a central database;

- Ensure autonomous and efficient recovery of a passenger's identification through these biometric procedures;

- Records the clearance of the passenger in order to maintain a log file on the individual's frequency of travel.[135]

With the badge that is issued from INM, the individual clears a first control process and must then authenticate his or her fingerprints on a scanner. Before authorizing the person

---

[134] ***Supra*** note 97 at page 6.
[135] ***Ibid.*** at page 4.

to clear border control, INM 's database conducts queries of criminals or delinquents, searches for false travel documents and gathers all information from different agencies around the world including consulates as well as Interpol. From these sources a "stop list" is generated for security purposes.

The difference between the Privium Dutch program and the Mexican Fast Track is that there are no means for a traveler to consult his or her personal file under the Mexican Fast Track system. However, under the terms and conditions of the Privium Program, a passenger can request the authorities to amend the information stored. Schipol Group could also be liable if found guilty of misuse of information. This is not the case for the INM Fast Track System.

The Mexican government suggested that although fingerprinting does not seem to be the most reliable form of biometric procedure recommended by IATA or SPT, it is the most cost-effective method.

Furthermore, it has been suggested that even though this system provides effective and efficient border control, more and more individuals seem to view it as a possible infringement of privacy:

"As described in the Introduction, businesses' ability to collect, process, store, and disseminate personal information is significant. This part explains the nature of the personal information industry and reviews accumulating evidence that American consumers are becoming increasingly concerned about their perceived loss of control over personal information"[136]

[136] William J. Fenrich, " Common Law Protection of Individuals Rights in Personal Information", (1996) 65 Fordham L.Rev. 951 at 14.

A more in-depth analysis of privacy rights over these new technologies will be further studied in the following chapter.

2.3.3 The German Approach to Biometrics ("Sicherungstechnik Program")

On January 1st 2002, The Bundeskriminalamnt, the Federal Criminal Police organization of Germany, amended their legislation[137] in order to allow specific biometric features such as fingers or hands and/or of face recognition to be added to an individual's passport. The collection of data has now been permitted under federal law on the condition that no central database be installed. In fact, the purpose of this new biometric feature is to allow authentication of such an individual's MRTD in order to facilitate the quick and efficient process for border control clearance.

The process is now currently being tested in Frankfurt's Rhein Main International Airport and is open to nationals who volunteer to adhere to this program. The traveler must then enroll at the passport office and all data that is to be added to the passport is kept with the Immigration authorities of the Bundesministerium des Innern, Ministry of Interior, where only the authorities concerned have access to this personal data.[138] At the preliminary

---

[137] *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz)* (Federal Criminal Police Act), (1 July 1997) online: < http://www.lrz-muenchen.de/~rgerling/gesetze/bkag_aus.html > (date accessed: 10 March 2003).

[138] Dr. Edgar Friedrich & Dr. Uwe Seidel, "Introduction of Biometrics in Travel Documents, Update On German Evaluation Activities", Fachbereich KT 43 Ausweise, Sicherungstechnik, BKA, 2002.

testing, which included approximately 200 individuals, face recognition was first introduced as a simple form of biometric procedure. Fingerprinting and iris recognition are now currently being tested in order to verify the degree of efficiency for confirmation of identification. To accomplish such a task, the German government immigration and federal police officials must continue to join efforts to prevent any leakage of information of stored data.

One of the main differences with the Privium system in the Netherlands's Amsterdam Schipol Airport and the German Program is that there are as of yet no provisions to control any misuse of information. Under Dutch law, liability occurs when an official is found guilty of willful misconduct regarding tampering of information or of gross negligence.[139] Therefore, provisions similar to the Bundesdatenschutzgesetzt, which regulates privacy rights and the usage of personal data, should be developed. For example, under general DE law, an individual charged with misappropriation of data could be found guilty and face imprisonment as well as a fine.[140] Such a provision could be added to the current German Program.

It would be therefore necessary to permit any traveler participating in the Sicherungstechnik Program to obtain a copy of all the information stored and the possibility for such an individual to request amendments to his or her current file, as

---

[139] ***Supra*** note 130.

[140] ***Supra*** note 136.

Privium already specifies. Currently, this Act would only permit such a person to refuse to participate to this program:

"[...] *whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;[...]*"[141]

The database in which each template will be currently compared for identification originates from databases of State Police. This authority creates a log of high- risk individuals based on prior convictions on a national basis. The system therefore creates a "central criminal database" to which no authority other than the Ministry of Interior has access.

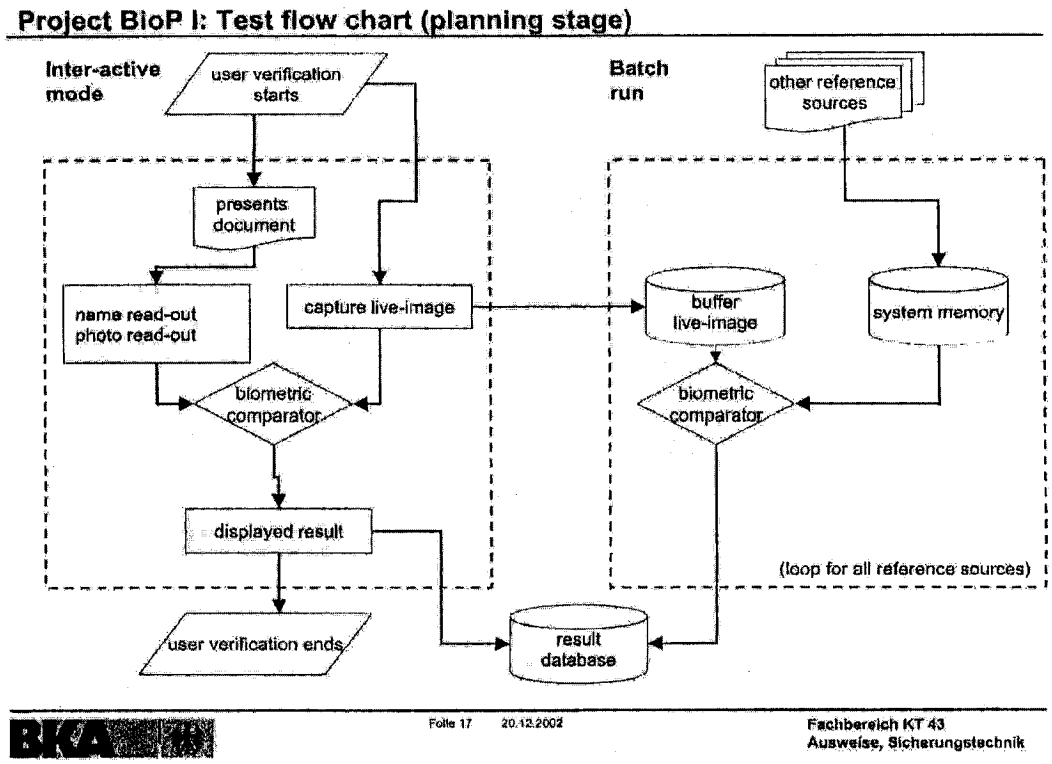
2.3.3.1 Illustration of the Sicherungstechnik Program

On the next page can be found an illustration of a typical processing of information that is carried out by the German immigration authorities. It basically can be summarized as:

- A sensor takes an original signature of an individual, either by fingerprinting, iris, or face recognition when the traveler procures his/her travel document in person;
- The system gives a normalized algorithmic version of the signature that is comparable to the one found on the travel document;

[141] ***Ibid.*** at article 30.

- A matcher reads the signature and compares it with the database containing the original signature taken when issuing the travel document and the one being currently used;
- As it authenticates the document, it searches in a database provided by the Bundeskriminalamt. It therefore verifies that no criminal file exist;
- When both verification of sources are done, the individual clears border control. The traveler may be still requested by the Bundesgrenzschutzpolizei, the border control inspectors, to present documentation for a secondary inspection.



In conclusion, although the German Biometrics Project is merely at a test level at present, it has proven to be helpful in the process of border control. [142]

[142] Interview of Mrs. Olivia Strese, representative of the Bundesministerium des Innern (German Ministry of Interior) (5 May 2003).

2.4 Problems to Be Encountered by Biometric Procedures

It could be suggested that such biometric procedures require strict terms, conditions and guidelines providing the passenger with the opportunity of consenting or not to such procedures. However, with or without these provisions, it may become mandatory in the future to possess personal biometric data in the MRTD as the United States and other Contracting States have indicated the need for stricter border access control and new technologies in order to achieve this.

One of the few problems to be encountered is the immature state of the art technology for certain biometric applications. Although, further tests are being conducted, such as the German Biometric Project, the time frame and level of accuracy is still not considered to be fully accurate for Contracting States. Privacy issues will be further dealt in the following chapter but as an introduction, the infringement of an individual's right to privacy represents a growing concerning biometric technologies. To quote Abeyratne:

"Legal issues pertaining to biometric identification of the airline passenger, in particular, issues of privacy and inadmissibility, have to be considered in advance, well before wide spread use of technology that would allow this method of identification to be a standard procedure at customs and immigration."[143]

Another concern is the labor issues that surround the usage of biometrics. For example, under the US *Enhanced Security Measures Act*[144], pilots may have to comply with new

[143] ***Supra*** note 118 at page 16.
[144] U.S., *Enhanced Security Measures Act*, Pub.L.No. 107-71, 115 Stat. 613 at section 109 (2001).

biometric procedures by being obliged to carry an encoded identification chip that would contain personal information thereby authenticating their identification:

"*Section 613: (6) In consultation with the Administrator of the Federal Aviation Administration, consider whether to require all pilot licenses to incorporate a photograph of the license holder and appropriate biometric imprints.*
(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation."[145]

With the implementation of such regulations, it is more likely than feasible that work relations may deteriorate as an individual's right to privacy may inevitably be violated. For example, Qantas had requested its ground workers to identify themselves with biometric procedures through fingerprinting, which provided to be unsuccessful. According to the Australian Industrial Relations Commission, the air carrier had to withdraw the implementation of these biometric procedures and resort to conventional methods such as time cards establishing between what times the employee was at work.[146]No progress on biometric procedures was made in this instance.

Biometrics represent a technologically advanced method where working together with MRTD can result in the less likelihood of security breaches at border control points. As the information is sent to the port of destination prior to arrival as API, biometrics can assist in the accuracy in identifying the traveler's MRTD.

[145] ***Ibid.*** at section 613 provisions 6 & 7.
[146] ***Supra*** note 58.

CHAPTER 3 : PRIVACY RIGHTS TOWARDS ADVANCE PASSENGER INFORMATION/PASSENGER NAME RECORD

The fundamental right of privacy is governed on principles of the right to be informed as to which public agency should be entitled to dispose of API and PNR information as well as the content of such data capturing in comparison with the State's recognized right to justify such a process under national security.[147]

This chapter will give an illustration of what could be considered to be the rights of a passenger concerning privacy issues and if it exceeds the criteria set forth by the Courts: the concept of *reasonable expectation*. It will further examine which guarantees must be given to prevent any infringements on these rights concerning API/PNR as well as biometrics. The chapter will also analyze the particular system of APIS in the United States.

---

[147] In this respect Dr. Ruwantissa Abeyratne has written:

> One of the issues as important in the API process is that the data required must be collectable by machine or already contained in the airline's system. Manual collection and data entry at the check-in desk for a scheduled flight is time-consuming and prone to errors, and or life. The foundations of "information privacy", whereby the individuals would determine when, how, and to what extent information about themselves would be communicated to others, inextricably drawing the right of control of information about oneself, is a cornerstone of privacy."

Dr. Ruwantissa Abeyratne "The Exchange Of Airline Passenger Information-Issues Of Privacy"(2001) Comm. Law Journal 6:5 at page 153.

1. PASSENGER RIGHTS

To illustrate the passenger rights pertaining to privacy, Abeyratne considers 3 specific criterias for these rights:

- *"the right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data;*
- *the right of an individual to know what data is disclosed, and what data is collected and where such is stored when the data in question pertains to that individual, the right to dispute incomplete or inaccurate data; and*
- *the right of people who have a legitimate right to know in order to maintain the health and safety of society and to monitor and evaluate the activities of government."*[148]

Most of these passenger rights find their essence in Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*:

"

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*[149]

In Europe, national legislations concerning protection of personal data were drafted in accordance with this Convention. The first criterion gives the right of privacy to personal life and family life. The access to PNR and API does in no way send information concerning the individual's personal life or family life; at most, data may be sent to border control authorities regarding the number of passengers traveling with the

---

[148] ***Ibid.*** at page 154.
[149] EC, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, (1950) online:<http://www.pfc.org.uk/legal/echrtext.htm > (date accessed : 7 April 2003)

individual. Furthermore, concerning the second criterion of the article, the transmission of information would be justifiable under the national security provision and public safety. In a statement given by the EC's Directorate-General for Energy and Safety Director, Dr. van Hasselt stipulates: "The Commission side emphasised its full solidarity with the US objective of preventing and combating terrorism and underlined the need for practicable solutions that would provide legal certainty for all concerned [...]"[150]

The EC Directive 95/46 stipulates the necessary guidelines that a State must adopt before the transmission of information can be sent out in a secure manner that respects the individual's right to privacy. Abeyratne quotes four main purposes:

"1) to create norms for collecting and processing personal data; 2) to provide an opportunity for affected individuals to renew information collected about themselves and to review the compiler's information practices; 3) to offer special protection for sensitive data, such as data pertaining to ethnic origins, religion, or political affiliation; and 4) to establish enforcement mechanisms and oversight systems to ensure that data protection principles are respected."[151]

As APIS and other API/PNR data are being currently used by different border control agencies, it would be necessary for the State handling such data to ensure that no leakage of information occurs as well as provide the passenger with an opportunity to consult his or her personal data. The EC Directive also gives in Article 22 the necessary legal tools required to remedy to breaches of privacy:

"Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any

---

[150] ***Supra*** note 67 at note 2 of joint statement.

[151] Pamela Samuelson, "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy", Book Review of *Data Privacy law, Study of the United States Data protection* by Paul M. Schwartz & Joel R. Reidenberg (1999) 87 Cal. L. Rev. 751 at 753.

breach of the rights guaranteed him by the national law applicable to the processing in question."[152]

The concept of privacy was also applied in Germany in a landmark case by the Constitutional Court, the German Bundesverfassungsgericht, in 1983.[153] This judgement was a study on the right of self-determination concerning private information of individuals being used by other authorities. The Court Senate determined that unless an individual is made aware of the data's usage, it could possibly infringe on the right of privacy, an aspect which cannot be tolerated in a democratic society.[154] Therefore, in order to fully comply with national laws pertaining to data protection, a standard should be established in order to advise air carriers which data is sent for border control clearance purposes. For example, die Deutsche Lufthansa Aktiengesellschaft, has already implemented an advisory in their website in order to advise the passenger of the data being collected and to what purpose it will serve. In this case, Lufthansa decided to format this advisory in a "Question-Answer" that submits all details to travelers wishing to inquire on this subject.[155]

---

[152] ***Supra*** note 65 at article 22.

[153] *Volkszählung (Self-determination)*, BverGE 65, 1 (Bundesverfassungsgericht-German High Constitutional Court) (1983).

[154] The text concerning usage of information of the self-determination German Decision reads as follows:

> [...] Zwar begrenzt die Bestimmung damit die Verwendung personenbezogener Einzelangaben im kommunalen Bereich auf statistsiche Aufbereitungen.[...] Eine derartige Sicherung ist insbesondere deshalb geboten, weil in vielen Gemeinden keine für die Bearbeitung von Statistiken zuständigen Stellen vorhanden sind, so daß eine ausschließlich für statistische Zwecke vorgesehene Nutzung der Daten nicht als ausreichend gewährleistet angesehen werden kann [...] .

Ibid.

[155] [Unpublished]

2. LEGAL FOUNDATION FOR COLLECTION OF DATA

Concerning the collection of data during border control clearance, it can find legal justification under Article 29 of the Chicago Convention which requires each aircraft engaged in international air transport to possess a list of the names of each passenger, their place of embarkation and destination. In addition to this, Annex 9 also specifies that information provided should include all data that can be found in the passenger's travel documents:

"3.34 [...] When specifying the identifying information on passengers to be transmitted, Contracting States should only require information that is found in the machine readable zones of passports and visas that comply with the specifications contained in Doc 9303 (series), Machine Readable Travel Documents.[...]"[156]

A an illustration of this principle, the current US legislation has added additional criteria to this collection of data in order to form API messaging. In this new US Act, section 115 stipulates:

"A passenger and crew manifest for a flight required under paragraph (1) shall contain the following information:
(A) The full name of each passenger and crew member.
(B) The date of birth and citizenship of each passenger and crew member.
(C) The sex of each passenger and crew member.
(D) The passport number and country of issuance of each passenger and crew member if required for travel.
(E) ***Such other information*** *as the Under Secretary, in consultation with the Commissioner of Customs, determines is reasonably necessary to ensure aviation safety.*[please note that that the underlined text has been made by the author of this thesis]"[157]

---

[156] ***Supra*** note 7 at R.P. 3.34.
[157] ***Supra*** note 5 at section 115.

3. THE CONCEPT OF PRIVACY AND "REASONABLE EXPECTATION"

The right of privacy can be defined, according to United States Judge Thomas M. Cooley, as the right to be left to one's self and extends to the right of an individual's personality.[158] Previously, the right of privacy was defined as the right of an individual to determine what information would be given about oneself and the control of who should receive this information and to what extent this data should be transmitted.[159] Privacy issues arose during the late 1800's in North America with the evolution of media publicizing personal issues concerning individuals. In a landmark case under civil law in Quebec, Canada, the concept of reasonable expectation of privacy was studied in depth.[160]

In this case, the Supreme Court indicated that the media did in fact have the right to privy themselves of information that could be considered of public interest. The party that perceived the breach of the right of privacy invoked the information spread of private information concerning the individual's possible membership in the Jewish Mafia. According to the Supreme Court of Canada, defamation of character where false information is used against an individual is a punishable offense according to the *Quebec Civil Code*[161]. One of the very first provisions of this legislation guarantees to all the obligation to respect one's private life: "Every person is the holder of personality rights,

---

[158] Samuel.D. Warren & Louis D. Brandeis, "The Right of Privacy" (1980) 4:5 Harv. L. Rev. 193 at 195.

[159] Joel R. Reidenberg, "Data Protection Law and the European Union's Directive : The Challenge for the United States : Setting Standards for Fair Information Practice in the U.S. Private Sector" (1995) 80 Iowa L. Rev. 423 at 425.

[160] *Snyder vs. Montreal Gazette*, [1988] 1 S.C.R. 494.

[161] *Quebec Civil Code*, S.Q., 1991, c.64.

such as the right to life, the right to the inviolability and integrity of his person, and the right to the respect of his name, reputation and privacy."[162] The Court therefore agreed with the petitioner that an individual does have the right to expect some form of privacy. However, Justice Beetz believed that the right of privacy depends greatly on a circumstantial basis when assessing such a breach. In fact, the petitioner in this case was a well-known person to society. Therefore, there was a legitimate reason to believe that a celebrity would inextricably face some form of exposure. In fact, the petitioner, when accepting a public career, accepted implicitly to give up a portion of his private life. Therefore, his reasonable expectation of privacy would not be the same as that of another average individual.

The purpose of this thesis is to examine what expectation a passenger should have with regard to his right to privacy when traveling. As Article 13 of the Chicago Convention states, the Contracting State of the port of entry can impose on the traveler, its formalities of border control clearance. The concept of reasonable expectation of privacy for a traveler becomes relative, as he or she must follow the clearance formalities set forth by a Contracting State.

In a landmark US Supreme Court case, *Roe vs. Wade*[163] of 1973, The Court examined the different types of privacy such as physical privacy, decisional privacy, communications privacy, territorial privacy and information privacy. Concerning the communications

[162] ***Ibid.*** at article 3.
[163] *Roe vs. Wade*, 410 U.S. 113 (**U.S.** 22 January 1973).

privacy , it addresses data transmission. The Court determined in this instance that the right to privacy is circumstantial and not absolute.

When data such as PNR is accessed by Customs Officials, in order to rule on privacy issues, one should follow the *Roe* case which determined that the infringement must be greater that the goal which it wants to achieve. Therefore, when a passenger travels and his reservation record may be accessed by airlines and customs, the Courts would have to determine the circumstantial evidence surrounding any breach of privacy regarding this communication/transmission.

According to US legislation, the US Bill of Rights also deals with privacy issues. In 1928, in the *Olmstead vs. United States*[164] decision, Justice Brandeis used the Fourth Amendment, which refers to unreasonable searches, to explain the right of privacy. His conclusions were that the State couldn't use unlawful intrusion as a breach of an individual's privacy. However, because of the circumstantial evidence surrounding the possible breach, it was ruled that wiretapping in itself did not constitute an attack on privacy or proof of an illegal search, because the end result was to determine if the individual was guilty or not of a crime. The Court also found that the theory of trespassing into an individual's private life was the foundation of a breach of privacy. Once again, the circumstantial evidence can outweigh an infringement of privacy d if it goes beyond the criteria of reasonable expectation.

[164] *Olmstead vs. United States*, 277 U.S. 438 (**U.S.** 4 June 1928).

In 1979, in the *Smith vs. Maryland*[165] case of 1979, the US Supreme Court was faced with a decision regarding the wiretapping of a telephone conversation. It had to rule on the possible infringement of an individual's personal life. In order to evaluate the actual expectation of privacy, the Court used a two-tier system. As Abeyratne cites as per the judgement:

"First, the Court analyzed whether the individual had a legitimate expectation of privacy. If that were to be the case, the court proceeded to examine whether society is prepared to recognize that expectation as reasonable, and whether the individual is entitled to be free from unreasonable government intrusion".[166]

This landmark case established that when a US Court of law establishes that the intrusion in an individual's private life affects the public interest of society, the reasonable expectation becomes more and more relative.

In 1998, another decision was rendered by the Supreme Court of the United States regarding what is to be considered "reasonable expectation" of one's privacy.[167] Justice Rehnquist determined that although a police officer had observed a criminal act being performed on an individual's property, the defendant, by committing it near a window, gave up his implicit right to privacy: "Accordingly any search which occurred did not violate the respondents' rights to security against unreasonable search since they had no legitimate expectation of privacy in the apartment. It followed that the Fourth Amendment had not been violated [...]"[168]

---

[165] *Smith vs Maryland (State of)* 442 U.S. 735 (**U.S.** 20 June 1979).
[166] ***Supra*** note 2 at page 11.
[167] *Minnesota v. Carter and another*, 5 BHRC 457 (**U.S.** 6 October 1998).
[168] ***Ibid.***

In Canada, the concept of reasonable expectation of privacy was also analyzed by the Supreme Court of Canada. In 1998, a judgement was rendered after evaluating an individual's right to privacy against an illegal search in regards to the *Canadian Charter of Human Rights* section 8: "Everyone has the right to be secure against unreasonable search or seizure."[169] The petitioner attempted to use the Charter of Rights regarding illegal seizure on one's person with his right to privacy. Under Canadian criminal law, no seizures can be performed if they infringe on a person's right to privacy. However, Justice Cory stipulated that one must evaluate the circumstantial evidence surrounding the possible violation of a fundamental right. In this particular case, a student that violates a school regulation may face a seizure of any prohibited goods. This exceeds the reasonable expectation of one's privacy: " As a student the appellant had a reduced expectation of privacy and, on the facts, C had reasonable grounds to believe that he was in breach of school regulations and that a search would reveal evidence of that breach."[170]

4. EUROPEAN POSITION

Much of the European position to defend the passenger's right to privacy is based on Article 8 of the Convention for the Protection of Human Rights. This particular legal disposition gives the individual right to privacy concerning personal and family life. In a recent 1998 decision by the European Court of Human Rights, the Court had the opportunity of evaluating under which circumstances this right to privacy constituted an

---

[169] ***Supra*** note 77.
[170] *M.v.R.*, 5 BHRC 474 (Supreme Court of Canada) (26 November 1998).

infringement beyond the reasonable expectation of privacy: *Kopp vs. Switzerland.*[171] The case involved the interception of a telephone conversation of a Swiss attorney regarding possible fraudulent activities.

The judgement stipulated that infringement on one's private life depended a great deal on the circumstantial evidence that surrounded the breach of right. Furthermore, it needed to be justifiable according to a three-tier system:

1) The violation should have to be justifiable according to national law;
2) If it passed the first test, the violation had to be in accordance with the law's objective of a respecting the condition of a democratic society and public safety;
3) The final criteria the Court evaluated is the seriousness of the breach of privacy.[172]

It ruled that telephone conversation interception, when authorities had no reasonable doubt to suspect the respondent of fraudulent activity, constituted violation of privacy. Therefore, concerning a passenger's name record locator number is sent along with API information, the question remains as to whether this constitutes a breach of reasonable expectation of privacy. However, when a passenger travels, his documents may be inspected and therefore, API transmissions and PNR access cannot constitute a breach of reasonable expectation of privacy.

In another decision by the EU Court of Human Rights in 1993, the Court ruled that the search of goods when crossing customs does not violate Article 8 of the Convention on

[171] *Kopp vs Switzerland*, 4 BHRC 277 (European Court of Human Rights) (25 march 1998).
[172] ***Ibid.***

Human Rights.[173] In fact, the majority ruled that because local French customs laws permit any inspection of documents in their Article 65(1), inspection does not breach the second section of Article 8 of the Convention of Human Rights:

"Customs officers with the rank of at least inspector (inspecteur or officer) and those performing the duties of collector may require production of papers and documents of any kind relating to operations of interest to their department [...]"[174].

Therefore, for national security reasons, senior ranking officials could be permitted to commit such inspections.

5. THE "NATIONAL SECURITY" JUSTIFICATION

Many international jurisdictions permit breaches of rights should they be justifiable under national security. In fact, under the previously cited Article 8 of the European Convention on Human Rights, it was stipulated that any breach of privacy that is a direct consequence of maintaining public order and national security is not to be considered an infringement on an individual's right to privacy.

In a 1996 judgement by the European Court of Human Rights, the Court ruled on the right of privacy involving a deportation order.[175] In this particular instance, Belgium had accessed data on the individual's activity in Morocco prior to his arrival in Europe. The

[173] *Funke vs. France*, (1993) 16 EHRR 297 (European Court of Human Rights).
[174] ***Ibid.***
[175] *C. v. Belgium* [1996] ECHR 21794/93 (European Court of Human Rights).

judge determined that the right of privacy did not supersede the criminal offense committed by the respondent:

"However, the Court reiterated that it was for the Contracting States to maintain public order, in particular by exercising their right, as a matter of well-established international law and subject to their treaty obligations [...] Such decisions could only interfere with a right protected under art 8 (1) so far as they were necessary in a democratic society and it was the Court's task to determine whether the deportation in issue struck fair balance between the relevant interests, namely the applicant's right to respect for his private and family life, on the one hand, and the prevention of disorder or crime on the other[...] The applicant's expulsion could not be regarded as disproportionate to the legitimate interests pursued and there was accordingly no violation of art. 8."[176]

This position was also confirmed in *Khan vs. United Kingdom*[177]. The Courts determined that circumstantial evidence played an important role in the establishment of a possible infringement of the right of privacy. Furthermore, if the breach could be justified for the interest of public order and national security, there was no violation to the right of privacy.

Therefore, it could be suggested that the right to privacy can be minimized when faced with a situation of interest of national security. Regarding API information that primarily is utilized for effective border control clearance, it can also be used to determine if an individual should or not be allowed to travel to a said State. Under current European, Canadian and American courts, the reasonable expectation of the right of privacy could be greatly reduced when faced with a situation of interest of national security.

---

[176] ***Ibid.***

[177] *Khan vs. United Kingdom*, 8BHRC 310 (12 May 2000) (European Court of Human Rights).

6 . PHYSICAL CHARACTERISTICS AND THE RIGHT OF PRIVACY

Another aspect previously discussed that surrounds the concept of privacy is the physical characteristics of an individual that can be used as proof in a court of law. The question of intrusion of privacy was widely discussed and debated. In *United States vs. Dionisio*[178], the Supreme Court of the United States considered that sample of voice recognitions should not be considered as breaches of the Fourth Amendment and do not constitute reasonable grounds for a claim of infringement of privacy.

According to the US legislation, physical characteristics of an individual have never been found to be considered as violations of the reasonable expectation of privacy. In *United States vs. Mara Aka Marasovich*[179], Justice Stewart of the US Supreme Court focused on the Dionisio case previously cited and reiterated the concept of reasonable expectation of privacy:

"The Government then petitioned the United States District Court to compel Mara to furnish the handwriting and printing exemplars to the grand jury [...]. Handwriting, like speech, is repeatedly shown to the public, and there is no more expectation of privacy, in the physical characteristics of a person's script than there is in the tone of voice [...][180]*".*

The Courts have ruled that a sample of a person's voice does not go beyond reasonable expectation of privacy. The legal position regarding biometrics would not necessarily surpass reasonable expectation of privacy and may be deemed necessary for national security when used to confirm the identity of the traveler.

---

[178] *United States vs. Dionisio* 410 U.S. 19 (**U.S.** 22 January 1973).
[179] *United States vs. Mara Aka Marasovich* 410 U.S. 19 (**U.S.** 22 January 1973).
[180] ***Ibid.***

Many organizations conclude that there may be a need to define different elements of data such as sensitive data and other types of data that may be necessary for transmission for API/PNR purposes in order to determine exclusions of private information. When traveling on an air carrier from point A to point B, in order to facilitate efficient border control, the States should consider that the transmission of API and possible access to PNR information could prevent unnecessary delays in airports and illegal entry of a passenger.

In conclusion, although an individual's right to privacy represents a global issue, it is to be implicitly expected that a traveler be faced with inspection once crossing borders and some information stored in his or her MRTD. In fact, under US law the Fourth Amendment gives the right to the government to protect itself by stopping individuals and examining the person crossing into the country.[181] The Aviation Security Biometrics Working Group also quotes: "When we transit our borders, therefore, the authorities can closely scrutinize our person and property in ways that they could not do in another setting."[182] Although many States possess national laws preventing issuing personal data on their nationals, Article 13 of the Chicago Convention imposes on any State the obligation to comply with local authorities for border control clearance.

---

[181] *US Constitution, Fourth Amendment*, online :
< http://caselaw.lp.findlaw.com/data/constitution/amendment04/ > (date accessed : 11 March 2003)
[182] ***Supra*** note 123 at page 21.

7. PRIVACY RIGHTS vs US APIS SYSTEM

Although privacy rights have become a growing concern for the traveler regarding the gathering of personal data and the access of such information by the port of arrival authorities and by possibly third parties, all carriers have complied with the US's New Aviation and Transportation Act on a short term basis. The European Commission however feels that on a long-term basis, resolutions should be found with the US Customs Service in order to fully satisfy both EC and American laws concerning more specifically Article 25.6 of the EC *Data Protective Directive*:

"25 (6). The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals [...]"[183]

This Directive requests that specific measures be taken by third party States in order to protect the information that is sent and to maintain the right of privacy. The following analysis will demonstrate that the US APIS and PNR System have taken appropriate measures on a short-term basis to both satisfy the national requirements of privacy and still be able to access vital information.

According to the statement given by US Customs during the short-term resolution project set forth in February 2003, the US Customs gives appropriate remedies and prevents any

[183] ***Supra*** note 65 at article 25.6.

unauthorized employees to have access to such information. Should there be any leakage of information, employees could face criminal prosecution:

"- Customs policy and regulations provide for stringent disciplinary action (which may include termination of employment) to be taken against any Customs employee who discloses information from Customs computerized systems without official authorization (title 19, Code of Federal Regulations, section 103.34);

-criminal penalties (including fines and imprisonment of up to one year) may be assessed against any officer or employee of the United States for disclosing confidential business information obtained in the course of his employment, where such disclosure is not authorized by law (title 18, United States Code, section 1905)[...]

-no other foreign, federal, state or local agency has access to PNR through Customs databases;[...]"[184]

Furthermore, the EU-US Discussion of February 2003 gives additional protection to the right of privacy by the fact that US Customs would not be able to transmit PNR information to other agencies unless it was of national interest.[185]

However, the European Commission has more recently expressed greater concern on behalf of its member States in order to comply with all national data protection legislation. In order to make proper recommendations, it has asked US Customs to:

"It was agreed that the information and undertakings to be provided would need to cover in particular: definition of the purposes for which the data will be used and limitation of use to these purposes; conditions and limits of data sharing and onward transfer; protection of data from unauthorized access; duration and conditions of data storage; additional measures for the protection of sensitive data; remedies for passengers, including possibilities to review and correct data held by US Customs; reciprocity."[186]

---

[184] ***Supra*** note 45 at Annex.

[185] The text of the Joint EU-US Statement regarding PNR reads as follows:

> [...]other law enforcement entities may specifically request PNR information from Customs and Customs, in its discretion, may provide such information for national security or in furtherance of other legitimate law enforcement purposes.

Supra note 45

[186] ***Ibid.***

After discussing the privacy issues with the European Commission General Directorate for Energy-Transport, these officials suggested the adoption of a provision within Annex 9 of the Chicago Convention, although a short-term agreement was reached with US Customs. This international standard would regulate which data should be sent, which is to be excluded, such as sensitive data, and which guarantees a third party State would have to give in order to prevent unauthorized access of information.[187]

In accordance with this, the short-term discussion between the US and the EU gives assurance that only dedicated customs personnel with special training shall have access to PNR information:

"[...] only certain Customs employees who have completed a background investigation, have an active, password-protected account in the Customs computer system, and have a recognized official purpose for reviewing PNR data may access PNR data through Customs electronic connection to an air carrier's reservation system[...]"[188]

According to IATA, that currently represents 274 members, API information is already stored in the travel document and is being voluntarily given in compliance with Annex 9. Data pertaining to API is very specific and can be, according to IATA, justifiable under Article 13 of the Chicago Convention giving power to the State of entry to regulate its formalities for border control clearance.[189]

---

[187] Interview of Mr. Timothy Fenoulhet, European Commission, Energy and Transport Directorate-General (April 2003).

[188] ***Supra*** note 45.

[189] Letter from IATA to US Customs (28 August 2002).

IATA has also considered the EC Directive 95/46 that limits the amount of personal data being transferred to a third party. In accordance with such a directive, it is necessary for the EU member States to receive confirmation that such private information be protected against being misused. In response to this directive, the US implemented in July of 2000, the Safe Harbour Principles that give some guidelines in order to inform members of the EU on the usage of such information. However, IATA notes that even though the US Customs Services prevail themselves of these Principles, all other American agencies requiring this information would also have to adopt the Safe Harbour Principles[190]. The European Civil Aviation Conference had raised this aspect of API with the US government and stated the possible violations against national and European law that air carriers will encounter when faced with the US data provision requirements.[191]

During the European Civil Aviation Commission's Conference (ECAC) One Hundred and Fifth Meeting of Directors General of Civil Aviation in 2002, the greatest concern was not API in itself but the fact that the voluntary MOUs had now become compulsory. In addition, the fines imposed if an aircraft would not comply and the possible landing right revocation to the US spurred much controversy. This debate has now subsided as airlines have come to the conclusion that the American market in the travel industry is necessary for their livelihood and agreements should be sought to protect data privacy. [192]

---

[190] ***Ibid.*** at page 3.

[191] European Civil Aviation Conference, *One Hundred And Fifteenth Meeting of Directors General of Civil Aviation*, 2002, ECAC Doc DGCA/115-DP/7.

[192] ***Ibid.***

CONCLUSION

Advance Passenger Information and Passenger Name Record have puzzled many on the legality of such information being transmitted or accessed. The European Union and many other Contracting States have vehemently opposed such transmission of data. The air carriers in general as well as their representative, IATA, have found many legal loopholes in such data collection. It could be suggested that any obligation from other Contracting State could be viewed as an extraterritorial application of law. Furthermore, ICAO has been faced with other challenges such as the data collection and new biometric technologies.

It could be recommended that international regulation be a remedy to such relatively new application of advance transmission of information regarding passengers entering a State and proceeding through border control clearance. It could also be suggested to adopt the position of the Courts. In fact, under the covenant of national security, any infringement of privacy rights must be evaluated in regards to the objective of each national legislation: the security of its citizens.

Together with MRTDs and biometrics, the benefits of API transmission and PNR access enable Border Control Authorities to identify potentially high-risk individuals and process passengers in an efficient manner. As the *Chicago Convention* stipulates, a Contracting State may exercise the formalities that it deems necessary in order to

accomplish border control process. Concurrently, the legal framework required by the State should attempt to effectively prevent or at the least reduce privacy right infringements.

During the Facilitation Meeting of IATA that took place on July 29th, 2003, the Department of Homeland Security of the United States mentioned that comments would be encouraged for the final drafting of a Final Rule that would encompass API and PNR. The outcome may change the industry's culture and understanding of travel. Harmonization should be the key element to seek in order to ensure inter-operability of API transmission and PNR access.

Although the debate presently remains, agreements should be sought in order to promote civil aviation's objective: ensuring due regard for the safety of navigation of civil aircraft.

BIBLIOGRAPHY

LEGISLATION

Access to Information Act, R.S. 1985, c. A-1

Annex 9 to the Convention on International Civil Aviation (Facilitation), 11th Ed. (Montreal: ICAO 2002).
Canadian Charter of Rights and Freedoms, Constitution Act, 1982, c.1.

Convention on International Civil Aviation, 7 December 1944, UN Doc. 7300/6 (1980)

Convention On the Simplification And Harmonization Of Customs Procedures, online:<http://www.unece.org/trade/kyoto/ky-01-e1.htm#Historica> (date accessed : 3 January 2003)**[Kyoto Convention]**.

EC, *EC Data Protection Directive (95/46EC), Protection of the individuals in relation to the processing of personal data*, (Brussels: EC,1995), online : < http://wwwdb.europarl.eu.int/oeil/oeil4.Res213 > (date accessed : 5 march 2003).

EC, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, (1950) online:<http://www.pfc.org.uk/legal/echrtext.htm > (date accessed : 7 April 2003

EC, *Initiative of the Kingdom of Spain with a view to adopting a Council Directive on the obligation of carriers to communicate passenger data*,[2003] O.J.L.82/23.

Freedom of Information Act, 5 U.S.C. § 552 (1996).

Immigration And Refugee Protection Act, L.c. 2001, c.27 **[IRPA]**.

German Federal Ministry of Interior, *Bundesdatenschutz*, (December 1990), online: <http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm#absch1 > (date accessed: 17 January 2003).

Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz) *(Federal Criminal Police Act), (1 July 1997) online:*< http://www.lrz-muenchen.de/~rgerling/gesetze/bkag_aus.html > (date accessed: 10 March 2003).

Machine Readable Travel Documents, ICAO Doc 9303 (2002) at II-2.

Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States of 2001, 66 Fed. Reg. 67482 (2002)..

Quebec Civil Code, S.Q., 1991, c.64.

U.K., H.C.,"UK Data Protection Act", (1998), online: <http://www.hmso.gov.uk/acts/acts1998/80029--d.htm#28 > (date accessed: 3 July 2003).

Passenger Name Record Information Required For Passengers On Flights In Foreign Air Transportation To Or From The United States, 67 Fed. Reg. 42710 (2002).
Privacy Act, R.S. 1985, c. P-21.

U.K., H.C., "House of Commons Standing Committee on Delegated Legislation Draft Immigration (Leave to Enter and Remain) Order", (2000), online: <http://www.hmso.gov.uk> (date accessed : 4 March 2003)

U.K., H.C.,"Regulatory Impact Assessment : Introduction to Extended Powers of Information Collection On Passenger and Goods, Schedule 7 to the Terrorism Act 2000 (Information Order)", (2002), online :
<http://www.homeoffice.gov.uk/atoz/pax_and_goods.pdf > (date accessed: 8 November 2002

U.K., H.C., "UK Anti-Terrorism, Crime and Security Act", (2001), online: <http://www.hmso.gov.uk/acts/acts2001/10024--n.htm#119 > (date accessed: 4 July 2003).

Switzerland, *Swiss Data Protection Act*, (19 June 1992), DSG SR 235.1.

U.S., *Air Transportation Security Act*, 49 U.S.C.S § 44903 (2002).

U.S., H.R. Con., *Aviation and Transportation Security Act*, 107th Cong., 2001

U.S., *Enhanced Security Measures Act*, Pub.L.No. 107-71, 115 Stat. 613 at section 109 (2001).

US Constitution, Fourth Amendment, online :
< http://caselaw.lp.findlaw.com/data/constitution/amendment04/ > (date accessed : 11 March 2003)

JURISPRUDENCE

C. v. Belgium [1996] ECHR 21794/93 (European Court of Human Rights).

Funke vs. France, (1993) 16 EHRR 297 (European Court of Human Rights).
Khan vs. United Kingdom, 8BHRC 310 (12 May 2000) (European Court of Human Rights)

Kopp vs Switzerland, 4 BHRC 277 (European Court of Human Rights) (25 march 1998)

Minnesota v. Carter and another, 5 BHRC 457 (**U.S.** 6 October 1998).
M.v.R., 5 BHRC 474 (Supreme Court of Canada) (26 November 1998).

Olmstead vs. United States, 277 U.S. 438 (**U.S.** 4 June 1928).
R. v. Gruenke, [1991] 3 S.C.R. 265.

Roe vs. Wade, 410 U.S. 113 (**U.S.** 22 January 1973).

Smith vs Maryland (State of) 442 U.S. 735 (**U.S.** 20 June 1979).

Snyder vs. Montreal Gazette

United States vs. Dionisio 410 U.S. 19 (**U.S.** 22 January 1973).

United States vs. Mara Aka Marasovich 410 U.S. 19 (**U.S.** 22 January 1973).

Volkszählung (Self-determination), BverGE 65, 1 (Bundesverfassungsgericht-German High Constitutional Court) (1983).

SECONDARY MATERIAL: AGREEMENTS

Smart Border 22 Point Agreement" *US White House* (21 March 2002), online:
< http://www.whitehouse.gov/infocus/usmxborder/22points.html > (date accessed: 8 July 2003).

US-Canada Smart Border/30 Point Action Plan, online : <http://wwww.whitehouse.gov/news/2002/12/20021206-1.html > (date accessed : 17 December 2002).

SECONDARY MATERIAL : ARTICLES

Abeyratne Ruwantissa Dr., "Biometric Identification Of Airline Passengers", [2002] Tolley's Comm. L.1.

Abeyratne Ruwantissa Dr., "Intellectual Property Rights And Privacy Issues-The Aviation Experience In API And Biometric Identification" (2002) **5:4** J.W.I.P. 632

Abeyratne Ruwantissa Dr., "The Exchange Of Airline Passenger Information-Issues Of Privacy"(2001) Comm. Law Journal 6:5 at page 153.

" Data Protection" *Frashfields Bruckhaus Deringer*, online: <http://www/freshfields.com/practice/ipit/publications/22367.pdf> (date accessed: 6 February 2003).

Dearne Karen, "Immature Biometrics ID Systems Flawed", *International Biometric Group* (3 March 2003), online: < http://www.biometricgroup.com/in_the_news/australian_it.html > (date accessed: 8 July 2003)

Fenrich William J., " Common Law Protection of Individuals Rights in Personal Information", (1996) 65 Fordham L.Rev. 951 at 14.

Friedrich Edgar Dr. & Seidel Uwe Dr., "Introduction of Biometrics in Travel Documents, Update On German Evaluation Activities", Fachbereich KT 43 Ausweise, Sicherungstechnik, BKA, 2002

Hardy Michael, "Group Issues Final Biometrics Report", (28 February 2003), online : Federal Computer Week < http://www.fcw.com/fcw/articles/2003/0224/web-bio-02-25-03.asp > (date accessed : 9 March 2003

McMunn Mary K., "Aviation Security And Facilitation Programmes Are Distinct But Closely Intertwined" ICAO Journal 51:9 (November 1996) 7.

Radwanski George, "Privacy Commissioner of Canada: News Release" (9 April 2003), online: < http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_2_e.as >(date accessed: 8 November 2002).

Reidenberg Joel R., "Data Protection Law and the European Union's Directive : The Challenge for the United States : Setting Standards for Fair Information Practice in the U.S. Private Sector" (1995) 80 Iowa L. Rev. 423 at 425

Samuelson Pamela, "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy", Book Review of *Data Privacy law, Study of the United States Data protection* by Paul M.
Schwartz Paul M. & Reidenberg Joel R. (1999) 87 Cal. L. Rev. 751 at 753.

Warren Samuel D. & Brandeis Louis D., "The Right of Privacy" (1980) 4:5 Harv. L. Rev. 193 at 195.

SECONDARY MATERIAL: AGREEMENTS

"Smart Border 22 Point Agreement" *US White House* (21 March 2002), online:
< http://www.whitehouse.gov/infocus/usmxborder/22points.html > (date accessed: 8 July 2003).

US-Canada Smart Border/30 Point Action Plan, online : <http://wwww.whitehouse.gov/news/2002/12/20021206-1.html > (date accessed : 17 December 2002).

SECONDARY MATERIAL: INFORMATIVE DOCUMENTS

Brochure from SPT (2002) "*Simplifying Passenger Travel*"

ICAO Secretariat, *MRTDs Optimizing Security and Efficiency*, ICAO Circular (2002).

INS, "INS Extends Enrollment Period", 2003, online:
< http://www.immigration.gov/graphics/publicaffairs/newsrels/sentriextent.htm > (date accessed: 9 March 2003)

Privium Program, "Terms and Conditions of Privium", 2003, online:
<http://www.schiphol.nl/schiphol/content/content_C_c_1.jsp?CONTENT%3C%3Ecnt_id=226867&FOLDER%3C%3Efolder_id=379167&guidenr=00&guidemode=vac&entry=90&bmUID=1047138237310&submenu=/Assortments/Main/Primary/Schiphol/General/menus/menu90/Algemene_Voorwaarden > (date accessed : 9 March 2003).

World Customs Organization, online: < www.wcoomd.org> (date accessed: 10th December 2002).

SECONDARY MATERIAL: LETTERS/ INTERVIEWS/ STATEMENTS

Interview of Mr. Timothy Fenoulhet, European Commission, Energy and Transport Directorate-General (April 2003).

Interview of Mr. Timothy Fenoulhet of the EC Commission's Energy and Transport Directorate (5 July 2003).

Interview of Mrs. Olivia Strese, representative of the Bundesministerium des Innern (German Ministry of Interior) (5 May 2003).

Joint Statement of the European Commission/ US Customs Talks on PNR Transmission (17-18 February 2003

Letter from Air 2000 Limited to US Customs (26 August 2002).

Letter from Air Transat to US Customs (28 February 2002).

Letter from American Airlines to US Customs (28 February 2002). Unofficial letter from Continental Airlines to US Customs (28 February 2002).

Letter from British Airways to US Customs (1 March 2002).

Letter from British Airways to US Customs (26 August 2002).

Letter from IATA to US Customs (26 August, 2002).

Letter from IATA to US Customs (28 August 2002).

Letter from the Deutsche Lufthansa Aktiengesellschaft to US Customs (30 August 2002).

Letter from the EC Directorate-General for Energy and Transport to US Customs (19 February 2003).

Letter from the Directorate-General for Energy and Transport of the EC to ICAO (18 June 2003).

Letter from Qantas Airways to US Customs (22 August 2002).

Letter from Swiss International Air Lines to US Customs (26 August 2002).

Letter from Varig's legal counsel to US Customs (18 September 2002).

Letter from Virgin Atlantic Airways Ltd. To US Customs (30 August 2002).

Unofficial statement given by Dennis Benjamin, US Customs Service (December 2002).

Unofficial interview of Francis Morgan of the European Commission (25 March 2003).

SECONDARY MATERIAL: PAPERS

Association of Asia Pacific Airlines, "Passenger Facilitation-A New World Order-2002 Annual Report", online: Association of Asia Pacific Airlines < http://www.aapairlines.org/content/annualreport/API.pdf > (date accessed: 7 January 2003

Australian Delegate to ICAO, *Facilitation Panel Fourth Meeting Information Paper*, 2002, ICAO Doc FAL/4-IP/8.

"Aviation Security Working Group Steering Group Analysis", 2001, online : <http://www.biometricscatalog.org/asbwg/Files/ASBWG_Steering_Committee_Analysis1.pdf > (date accessed : 9 March 2003).

European Civil Aviation Conference, *One Hundred And Fifteenth Meeting of Directors General of Civil Aviation*, 2002, ECAC Doc DGCA/115-DP/7.

ICAO Secretariat, *Eleventh Session Information Paper On Advance Passenger Information (API) Guidelines Adopted by the WCO*, 1995, ICAO Doc FAL/11-IP/2 at point 3.

ICAO Secretariat, *Final Report Of The Second Session of the Facilitation Division*, 1948,

ICAO Doc 5464-FAL, 535.

ICAO Secretariat, *Informal Facilitation Area Meeting in Consultation with ACI on Advance Passenger Information*, 1997, ICAO Doc INF/FAL/DJE WP/11

ICAO Secretariat, *Information Paper: Facilitation Programme Support For Aviation Security-Submitted During The High-Level, Ministerial Conference On Aviation Security*, 2002), ICAO Doc FALP/4-IP/3.

ICAO Secretariat, *Report of the Eleventh Session of the Facilitation Division,* 1995, ICAO Doc 9649 FAL/11.

ICAO Secretariat, *Report of The Tenth Session of the Facilitation Division*, 1988, ICAO Doc 9527- FAL/10, 54.

ICAO Secretariat, *Working Paper on Advance Passenger Information Further Development of ICAO Doctrine*, 2002, ICAO Doc FALP/4-WP/2
WCO/IATA/ICAO, *Guidelines on Advance Passenger Information (API)*, WCO Annex I to Doc. PC0123E1 (2003).