Automation in Facilitation of Air Transport

BY

ALEJANDRO J. PIERA

Faculty of Law
Institute of Air and Space Law

McGill University, Montreal

August 2000

A Thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Masters of Laws (LL.M.)

Dedicated to my parents, Jesus and Maria;
my grandfather, Joaquin Rogelio; and
my sister, Maria Nydia

ABSTRACT

The air transport industry is at present subject to dramatic traffic growth, which is expected to triple in the next 20 years. The industry must attempt to meet this unavoidable challenge by somehow accommodating the increase in passenger flow. This thesis proposes to examine how automation devices may assist in meeting this challenge by facilitating passenger clearance. They would do so by improving the lengthy, formalistic, and overly-bureaucratic, immigration and customs procedures. A myriad of different legal issues are engaged by these initiatives. Although many of them are mentioned throughout this thesis, the core legal analysis focuses on the challenge to privacy triggered by these endeavours, and the conflicting interests of individuals and industry players. Finally, a proposal to eliminate, or at least to reduce, this conflict is recommended.

RÉSUMÉ

L'industrie du transport aérien est actuellement sujette à une croissance considérable du trafic, qui est censé tripler dans les 20 prochaines années. Cette industrie doit tenter de faire face aux inévitables défis qui accompagneront cette augmentation en s'adaptant d'une manière ou d'une autre à la croissance du flot de passagers. La présente thèse propose d'examiner de quelles manières les instruments automatisés peuvent aider à répondre à ces problèmes en facilitant l'acceptation de passagers. Cela passera par l'amélioration les procédures douanières et d'immigration, qui sont actuellement trop longues, formalistes et excessivement bureaucratiques. Une multitude de questions légales se posent dans ce domaine. Bien que la plupart d'entre elles soient traitées dans la présente thèse, l'analyse juridique principale sera centrée sur le problème de l'atteinte à la confidentialité causée par les questions sus-mentionnés, ainsi que sur les intérêts conflictuels des individus et des acteurs de l'industrie. Enfin, une solution pour éliminer, ou à tout le moins réduire ces conflits sera proposée.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the people who have remained with me through my whole existence; my parents, for having inculcated me the value of hard work, determination, persistence, and perseverance, but above all for positively criticising my life, thereby reminding me that I do not possess the absolute truth of my acts; my grandfather, for being a continuous source of inspiration, and for believing in every single one of my projects; my sister, for her never-ending support and computer knowledge assistance in the darkest nights. If I lived up to your expectations, that will be my greatest achievement.

I am indebted to my supervisor, Prof. Dr. Michael Milde, for his invaluable support, constant encouragement, and genuine guidance in supervising this thesis. His famous "open door" policy has provided me with a unique opportunity to enlarge my limited knowledge, not solely within the field of law, but rather on a myriad of topics. I have enormously enriched my life through his intellectual philanthropy.

I am very grateful to Mr. Jitendra Thaker, Senior Official of ICAO, for discussing and commenting on my thesis on numerous occasions, and for giving me access to uncountable documents and sources. I must also thank my colleague and friend Eduardo Julian Hermida for taking the time to read and discuss my thesis; interminable juridical chats that led to significant conclusions.

I acknowledge the financial support of McGill University Graduate Programmes in Law for awarding me a triple differential fee waiver. I especially thank the Universidad Nacional de Asuncion for giving me the Rectorado Scholarship, despite the political and economic turmoil that my country Paraguay has been experiencing. I also express my appreciation to Mrs. Margaret Baratta, who gave me numerous part-time assignments that enabled me to subsist, particularly when my personal budget started shrinking.

My grateful thanks go to: Mrs. Viljane Ritva, Director of the Finnish Population Centre, who kindly assisted me with the Finnish smart card initiative; Mr. Jan van Arkel, Director of the National Chipcard Platform, who considerately explained the Dutch smart card approach; Mrs. Julie Plante, E-Ticketing Manager of Air Canada, who provided me with the insight view of air carriers; Mr. Louis Haeck, Senior Official of IATA, who gave me

access to several statistical sources; George Forbes and Harold Lapin, staff of the Nahum Gelber Law Library, who helped me with all the legal research.

I would like to express my gratitude to: Miguel Arnaldo Canale Frescura, my childhood friend and professional partner, whose loyal support and understanding has meant so much in the past twenty years of my life; Patricia Vitale, for putting up with our differences, but still believing in my projects; Mariana Flecha, for being simply Mariana Flecha and allowing me to discover new facets of my personality; Jesus Maria Sanchez, for helping to prepare for my stay in Canada, for never stop dreaming about a better future, and especially for keeping me optimistic in the obscurest hours; Lissette Ibanez, for generously arranging my travel flights; Mrs. Cora Montorfano de Blanco, for introducing me to the fantastic world of credit cards; Mr. Carlos Perez, for making me aware of the existence of the IASL programme; Professor Dr. Sindulfo Blanco, for inspiring in me the passionate feeling of law when certainly I was not finding it. I owe just as much to Silvia Albertini, whose encouragement, guidance, and friendship on an earlier working assignment installed in me the passion for the aviation industry. Without her help, I would have probably quit.

I would also like to recognise all the love and support that I have received from my American family, "the Loomis's", who have been an inspirational source ever since we met. I also acknowledge all the efforts undertaken by Lars Peter Nelsen, Hugo Villadavel, and Tevin Pathareddy to keep me away from insanity.

I assert my appreciation to: Fabienne Vandenabeele, who not only translated my abstract to French, but also has been a cheering friend throughout the year; and Melissa Knock, who expeditiously edited this thesis, encouraged me to continue, and coped with all my demanding requests. Mrs. Carol Loomis and Mr. Adam Kramer also removed linguistic ambiguities.

Last but not least, I would like thank all the members of the McGill LL.M. class of 1999/2000, the people who made this experience in Montreal, Canada an unforgettable one, specially: Alfredo Gomez-Perez, Maria Eugenia Cambur Salazar, Claudio Andres Luqui, Juan Martin Jovanovich, Jose H. Frias, Hodjat Khadjhavi, I. Amana, Carlos de Icaza, Claudia Sarrocco, Ernesto Rodriguez, and Burcu Inal

Thank you all! The shortcomings remain all mine.

TABLE OF CONTENTS

Abstract I
Résumé II
Acknowledgements III
Table of Contents V

Introduction
Emerging Trends in Air Transport

I. Air Traffic Growth 1
II. The Shifted Paradigm in Air Transport 3
III. An Alternative Approach to the Increasing Air Traffic Growth 4

Chapter One
International Civil Aviation Organisation Facilitation Programme

1.1. The Chicago Convention 6
1.2. Annex 9 7
1.3. Conflict of Interest – Facilitation vis-à-vis Drug Trafficking and Security 16

Chapter Two
Cutting Red Tape

2.1. Machine Readable Travel Documents 20
2.1.1. Machine Readable Passports 21
2.1.2. Machine Readable Visas 22
2.1.3. Machine Readable Official Travel Documents 23
2.1.4. Machine Readable Crew Member Certificates 23
2.2. Advance passenger Information (API) 24
2.3. Smart Cards 27
2.3.1. European Smart Card Initiatives 29
2.3.1.1. The Dutch Initiative 30
2.3.1.2. The Finnish Initiative 30
2.3.1.3. Applications to Air Transport 32
2.3.1.4. Critical Appraisal 33
2.3.2. Biometric Applications in Smart Cards 33

2.3.2.1. Biometric Scanning 34
2.3.2.2. Applications to Air Transport 35
2.3.2.3. Critical Assessment 35
2.4. Smart Cards Applications to Air Transport 36
2.4.1. Air Carriers' Endeavours 36
2.4.2. US INSPASS 38
2.4.3. CANPASS 39
2.4.4. Simplifying Passenger Travel 40
2.5. Global Assessment of Automation Initiatives 44

Chapter Three
Banking, Financial, and Evidentiary Issues

3.1. Banking, Financial, and Consumer Law Implications 46
3.1.1. Credit Cards *vis-à-vis* Debit Cards 47
3.1.2. Unauthorised Uses 48
3.1.3. Regulation E 50
3.1.4. Regulation Z 51
3.2. Inadmissible Passengers 52
3.3. Critical Assessment 55

Chapter Four
Privacy

4.1. The Shifted Paradigm of Privacy. Towards a Traceable Society? 56
4.2. The International Recognition of the Right of Privacy 58
4.2.1. OECD Guidelines 58
4.2.2. United Nations Guidelines 59
4.3. The Concept of Privacy 60
4.4. Privacy in the United States 62
4.4.1. Privacy Dimensions 65
4.4.2. Public Sphere of US Privacy Laws 66
4.4.2.1. United States Federal Statues 71
4.4.3. Private Sphere of US Privacy Laws 72
4.4.3.1. The Law of Torts 73
4.4.3.2. United States Private Sphere Statutes 76
4.4.4. United States Privacy Law Critical Assessment 78
4.5. The European Privacy Approach 79
4.5.1. The European Privacy Data Protection Directive 81
4.5.1.1. Objective 81
4.5.1.2. Scope of Application 82
4.5.1.3. Jurisdiction 83
4.5.1.4. Quality of Data Processed 84

4.5.1.5. Unambiguous Consent Principle 84
4.5.1.6. Processing of Sensitive Data 87
4.5.1.7. Data Subject's Bill of Rights 87
4.5.1.8. Legal Remedies 89
4.5.1.9. Transborder Data Flows 90
4.5.1.10. EC Directive's Flaws 93
4.5.1.11. EC Directive's Code of Conduct 94
4.6. The Canadian Privacy Data Protection Approach 95
4.6.1. Private and Public Privacy Spheres 95
4.6.2. The Emergence of a *Suis Generis* model 97
4.6.2.1. The Personal Information Protection and Electronic Documents Act 98
4.6.2.1.1. The "Reasonable Collection, Usage, and Disclosure" Principle 100
4.6.2.1.2. The "Consent and Knowledge" Principle 100
4.6.2.3. Transborder Data Flows 102
4.6.3. Critical Assessment 103
4.7. The Conflict over Privacy Data Protection Ideologies: Insuperable Legal Hurdles for Transborder of Data Flows? 104
4.8. An Alternative Proposal to Transborder Data Flows in Air Transport 106
4.9. Privacy Assessment 111

CONCLUSION 113

BIBLIOGRAPHY 115

Emerging Trends in Air Transport

In 1944 the memorable Douglas DC-3 carried 28 passengers at a speed of 320 kilometres per hour with an autonomy range of 3,400 kilometres. Although an outstanding aircraft for its time, with the advent of the jet era in 1958 the DC-3 it was drastically outperformed by the revolutionary B-707-the commercial jet aircraft substantially reduced costs while improving fuel efficiency, and speed in air transportation.[1] By 1969 the magnificent double-decker B-747 was soaring the skies. Today its latest model, the 747-400, is able to transport 524 passengers with an autonomy range of 8,400 miles flying at approximately 900 kilometres per hour.[2] Meanwhile, Airbus Industrie has conducted numerous studies to develop a design for a wide-body aircraft integrating the most advanced technologies. The result is a double-decker jumbo -cruise ship- Airbus A3XX-100[3] that will be capable of carrying 555 passengers in a standard three-class configuration. This aircraft will offer 15 to 20% lower operating costs compared to the B-747-400, while providing up to 35% more seats and 10 to 15% more range.[4]

I. Air Traffic Growth

It is estimated that there are approximately 10,000 aircraft in the air at any given time.[5] The world fleet will need 8,900 additional aircraft over the next decade, which means

[1] Pan American World Airways inaugurated transatlantic B-707 jet service between New York and Paris with a capacity of 120 passengers. See Boeing, "707 Family" online: http://www.boeing.com/commercial/707family/index.html (date accessed: 20 June 2000).

[2] See Boeing, "747-400 Family" online: http://boeing.com/commercial/747-400/family/index.html (date accessed: 20 June 2000). See also Boeing, "747-400 Specifications" online: http://boeing.com/commercial/747-400/product.html (date accessed: 20 June 2000).

[3] See D. Seward, "Airbus Announces 555-Seat Plane" *Associated Press* (23 June 2000), online: http://biz.yahoo.com/apf/000623/france_air_7html (date accessed: 23 June 2000).

[4] See Airbus Industrie, News Release "A3XX Receives Authorisation to Offer" (23 June 200); "ILFC Interested in the A3XX" (7 June 2000), online: http://www.airbus.com/media/press.asp http://www.airbus.com/media/press.asp (date accessed: 23 June 2000). Airbus is also designing the A3XX-200 and the A340-600, which are expected to hold 700 and 400 passengers respectively. See Airbus, "A3XX Commonality" online: http://www.airbus.com/products/A3XX_commonality.html http://www.airbus.com/producs/A3XX_commonality.html (date accessed: 20 June 2000).

[5] See ICAO, *Outlook for Air Transport to the Year 2003* (Montreal: ICAO, 1995) at 5.

there will be an amazing 18,900 aircraft flying by the year of 2008.[6] The demand for new equipment is reflected in air traffic growth, which is directly linked to economic growth. Hence, Boeing's current 10-year market outlook estimates that worldwide economic growth will average 2.7% per year, passenger traffic growth will average 4.7% per year, and cargo traffic will increase at 6% per year.[7] According to Boeing's 1999-2018 forecast, the most rapid air traffic growth is expected in the Asia-Pacific region at a pace of 6.1% per year, followed by Africa at 4.9%, Latin America at 4.5%, Europe at 4.3%, the Middle East at 3.9%, and North America at 3.7%.[8] World air traffic will then triple in the next 20 years.[9] Airline yields are expected to increase at an average annual rate of 0.5% in the next 5 years.[10]

In 1999, IATA member airlines carried over 1.3 billion passengers and 27.7 million tonnes of cargo representing a growth of 3.8% and 5.9% from 1998 respectively.[11] As pointed out by Mr. Pierre J. Jeanniot, Director General and CEO of the International Air Transport Association (IATA), the world scheduled air transport industry has grown from an estimated 9 million passenger journeys in 1945 to about 1.5 billion in 1999, and the volume of cargo carriage by the world's airlines has risen from a few thousand tonnes in 1945 to 25 million tonnes today. By 2010, the number of passenger journeys by air could exceed 2.3 billion. Passenger and freight traffic will increase at an average annual rate of 5% between 1999 and 2010, a rate considerably greater than that of the growth of the global Gross Domestic Product.[12] The disparity between these two rates of growths has significant consequences for a large number of countries, which may not be in a financial position to

---

[6] See Boeing, "Worldwide Airplane Deliveries" online: http://www.boeing.com/commercial/cmo/4wa01.html (date accessed: 20 June 2000).

[7] See Boeing, "Current Market Outlook, Executive overview" online: http://www.boeing.com/commercial/cmo/1eo01.html (date accessed: 20 June 2000).

[8] See Boeing, "Current Market Outlook, Results by Region of the World" online: http://www.boeing.com/commercial/cmo/5apc1.html (date accessed: 20 June 2000).

[9] See Airbus, "A3XX Economics" online: http://www.airbus.com/products/A3XX_economics.html (date accessed: 20 June 2000). Accordingly, for instance, authorities from the San Francisco Bay area are predicting that air traffic for that particular region will double in the next 20 years. See Metropolitan Transportation Commission, "Aviation Forecasts Show Air Passengers Double by 2020" online: http://biz.yahoo.com/prnews/000712/ca_future_html (date accessed: 13 July 2000).

[10] See *supra* note 5 at 1.

[11] See IATA, *World Air Transport Statistics* (Montreal: IATA, 2000). See also IATA, News Release PS/12/00 "2000 W.A.T.S. – More Passengers, Less Profits" (19 June 2000), online: http://www.iata.org/pr/pr00jung.html (date accessed: 20 June 2000).

[12] See P. J. Jeanniot, "The Future of the Airline Industry" (Economist Global Airlines Conference, 16 May 2000), online: http://www.iata.org/pr/speech2.html (date accessed: 20 June 2000). See also IATA, News Release No. 13 "Customer Service, Liberalisation, and E-Commerce at Top of Airlines' Agenda" (6 June 2000), online: http://www.iata.org/pr/pr00junc.html (date accessed: 20 June 2000).

cope with the emerging burdens that come with air traffic growth. It has been estimated that a US$ 350 billion investment in air transport infrastructure, services, and en-route facilities will be needed to lodge the air traffic increase.[13] Even the Organisation for Economic Co-operation and Development (OECD),[14] an international body gathering the most industrialised nations of the world, recently noted that only about a fifth of its members are experiencing growth of their Gross Domestic Products.[15]

II. The Shifted Paradigm in Air Transport

The air transport arena has completely changed from its rather simplistic beginnings, wherein air travel, regarded as ultra-hazardous, was primarily a point-to-point activity reserved for the wealthy. With deregulation, liberalisation trends, and major private entrepreneurial intervention, the paradigm[16] has radically shifted, making air travel more accessible to the general public. This is reflected by rapid air traffic growth.[17] However, the aforesaid escalation of air transport requires major changes to the scenario faced nowadays. As a result the industry requires adequate infrastructure and services to cope with rapidly emerging trends.[18] Furthermore, the growth of air transport will still rely on four major factors: a) world economic and trade growth; b) air transport industry cost reductions; c)

---

[13] See ICAO, *Investment Requirements of Aircraft Fleets and for Airport and Route Facility Infrastructure to he Year 2010* (Montreal: ICAO, 1995).

[14] The OECD was created by the *Convention establishing the Organisation for Economic Co-operation and Development*, 14 December 1960, Paris, France [hereinafter *OECD*]. Its current members are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, France, Finland, Germany, Greece, Korea, Hungary, Iceland, Ireland, Italy, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

[15] See OECD, First Report on the OECD Growth Project, *Is there a New Economy?* (12 June 2000), online: http://www.oecd.org/subject/growth/new_eco.pdf (date accessed: 13 July 2000).

[16] The word paradigm is used in this thesis to refer to a period where science is looked at in a new way due to the emergence of new phenomena, a meaning denoted by Thomas S. Kuhn in *The Structure of Scientific Revolution* (Chicago: University of Chicago Press, 1962).

[17] See generally A. Kahn, "Airline Deregulation – A Mixed Bag, But a Clear Success Nevertheless" (1988) 16 Transp. L.J. 229 at 248; Organisation for Economic Co-operation and Development, *Deregulation and Airline Competition* (Paris: OECD, 1988) at 54; *The Future of International Air Transport Policy* (Paris: OECD, 1997) at 115; G. Williams, *The Airline Industry and the Impact of Deregulation* (Brookfield, Vermont: Ashgate, 1993) at 139; K. Button, ed., *Airline Deregulation, International Experiences* (New York: New York University Press, 1991) at 36. For an opposite argumentation on the positive impact of air transport deregulation, see *contra* M. Brenner, "Airline Deregulation – A Case Study in Public Policy Failure" (1998) 16 Transp. L.J. 179; M. Brenner, "Rejoinder to Comments by Alfred Kahn" (1988) 17 Transp. L.J. 253; P.S. Dempsey, "Airline Deregulation in the United States: Competition, Concentration, and Market Darwinism" (1992) XVII:I Ann. Air & Sp. L. 199 at 261.

[18] See ICAO, *The Convention on International Civil Aviation. Annexes 1 to 18* (Montreal: ICAO, 1991) at 17.

attention to such relevant issues as airport congestion, environmental protection, and high capital investment needs; and d) the development of facilitating automation mechanisms.[19] Simply, it is not feasible, or practical, to triple the current infrastructure to accommodate such increase in air transport. In addition, countries will not have the economic strength to confront those challenges.[20]

III. An Alternative Approach to the Increasing Air Traffic Growth

A variety of alternatives have been considered by different *fora* as viable solutions to cope with air traffic growth, *inter alia*, the establishment of an International Aeronautical Monetary Fund.[21] Nevertheless, one unequivocal way to confront the problem would be to implement automation[22] mechanisms and devices to facilitate the flow of air traffic, focusing on the clearance of customs lines and immigration passport controls' endless formalities.

Consequently, this thesis will thoroughly analyse the legal consequences of studies and programmes undertaken by numerous organisations seeking to implement automation methods through which facilitation in air transport could ultimately be achieved. Moreover, this thesis will demonstrate that automation in facilitation of air transport consists of a two-fold interrelated component: 1) the public facet, and 2) the private facet. The former encompasses the endeavours undertaken particularly under the patronage of the International Civil Aviation Organisation (ICAO), and the efforts to implement its Facilitation Programme's objectives in Air Transport through its Contracting States. The latter comprises the initiatives from the private entrepreneurial industry sector, which consist of a myriad of different actors, including air carriers, IATA, and banking institutions. Thus, Chapter 1 will critically examine the public facet of facilitation in air transport with particular

---

[19] See G.O. Eser, "Impact of Automation on the Airline Business" (1986) 11 Ann. Air & Sp. L. 3 at 5.
[20] See OECD, *supra* note 15.
[21] Although originally conceived for the development of satellite-based Communications, Navigation, Surveillance/Air Traffic Management (CNS/ATM), the foreseeable role of the International Aeronautical Monetary Fund has been extended to included aviation security and the development of proper infrastructure to cope with air traffic growth. The idea was originally proposed by the Latin American Civil Aviation Commission (LACAC) in 1994. It envisages the collection of an additional one US$ per passenger ticket sold. See R.I.R Abeyratne, "The Latin American Initiative Towards Funding the CNS/ATM System" (1998) 2 Aviation Q. 151; R.I.R. Abeyratne, "The Proposed International Aeronautical Monetary Fund – Legal and Practical Implications" (1998) 3:1 J. Air Transportation World Wide 1.

emphasis on the legal framework created by the Chicago Convention and the endeavours undertaken by ICAO to implement its facilitation programme under Annex 9; its merits, flaws, and conflictive interests will be carefully addressed. Chapter 2 will cover the "cutting red tape" initiatives of both the public and the private sectors aimed at achieving smoothness in passenger traffic flows. Particular emphasis will be placed on describing the initiatives on Machine Readable Travel Documents, Advance Passenger Information Systems, Smart Cards, and Biometrics, whereby an assessment of their global application will be provided. Chapter 3 will tackle banking, financial, and evidentiary issues that some of these initiatives compromise. Chapter 4 will provide the core legal analysis of this thesis by concentrating on the issue of privacy that all the endeavours herein described raise. Finally, a conclusion with some recommendations will be established.

[22] The word automation in this thesis will be used as "a means of processing and controlling great masses of varied data from many sources". I.H. Ph. Dideriks-Verschoor, "Automation and Air Law" (1987) XII Ann. Air & Sp. L. 15.

Chapter One

International Civil Aviation Organisation Facilitation Programme

1.1. The Chicago Convention

On 4 April 1947 the Convention on International Civil Aviation[23] entered into force and therewith the International Civil Aviation Organisation (ICAO) aimed at developing the principles, planning, and techniques of international air navigation, as well as ensuring safety and encouraging the development of airports and navigation facilities for international civil aviation.[24] Several articles in the Chicago Convention, the backbone of international civil aviation, are directly devoted to facilitation of air transport. For instance, Article 10 specifies that every aircraft entering the territory of another Contracting State must land at and take off from airports designated by that State in order to comply with customs examinations.[25] Article 11 provides that an aircraft entering or leaving a particular Contracting State must comply with the laws and regulations related to admission and departure thereof.[26] These formalities must be complied with, upon entrance into or departure from, or while within the territory of that state.[27] By adopting Article 22, Contracting States have agreed to adopt all practicable measures to facilitate and expedite the navigation of aircraft between their territories, avoiding unnecessary delays to aircraft, crews, passengers, and cargo, specifically when applying laws relating to immigration, quarantine, and customs.[28] Thus, each Contracting State is committed to developing customs and immigration procedures related to

---

[23] See *Convention on the International Civil Aviation*, 7 December 1944, 15 U.N.T.S. 295, ICAO Doc. 7300/6 [hereinafter *Chicago Convention*].
[24] See *ibid.*, art. 44.
[25] See *ibid.*, art. 10.
[26] See *ibid.*, art. 11.
[27] See *ibid.*, art. 13.
[28] See *ibid.*, art. 22. Accordingly, ICAO has urged Contracting States to give special attention to obligations established in the aforesaid article particularly aimed at providing the legal foundation for implementing its facilitation programme. See ICAO, *Consolidated statement of continuing ICAO policies in the air transport field*, Assembly Resolution A32-17, app. D (October 1998), online: http://www.icao.int/icao/en/res/a32_17.html (date accessed: 23 August 2000).

international navigation, "so far as it may find practicable", in accordance with the standards and practices established by ICAO.[29]

Pursuant to its objectives, the Chicago Convention provides that "[e]ach Contracting State undertakes to collaborate in securing the highest practicable degree of uniformity in regulations, procedures, standards, practices, and organisation in relation to aircraft, personnel, airways, and auxiliary services in matters in which such uniformity will facilitate and improve air navigation."[30] Thus, ICAO[31] has been bestowed the mandate to adopt and amend from time to time international standards, recommended practices, and procedures dealing with a vast variety of areas, *inter alia*, customs and immigration procedures.[32] Therefore, as stipulated under Article 54(l) of the Chicago Convention, ICAO elaborates the so-called "Annex" to implement those international standards and recommended practices adopted with the "consensus" of the Contracting States. The denomination of "Annex" was given purely for purposes of convenience.

1.2. Annex 9

Designated as "Annex 9", the Standards and Recommended Practices on Facilitation were originally adopted on 25 March 1949 and have since then been successively and comprehensively amended. The Tenth Edition of Annex 9, which came into force on 31 August 1997, contains provisions that originated in the Eleventh Session of the Facilitation Division held in Montreal in April 1995. While involving fairly diverse players such as civil aviation authorities, airport administrators, airline operators, regulatory authorities, and passengers, the term "facilitation" denotes the implication in air transport of a balkanisation of players, *inter alia*, customs, immigrations, agriculture, health, and tourism.[33] The complexity

---

[29] The words in quotation marks conceive the flexible discretionary safety net for Contracting States in cases where they may not be in a position to comply with such provisions. See *Chicago Convention*, *supra* note 23, art. 23.

[30] *Ibid.*, art. 37.

[31] For a comprehensive study on the law-making function of ICAO, see T. Buergenthal, *Law Making in the International Civil Aviation Organisation* (Syracuse, New York: Syracuse University Press, 1969). See also J. Ducrest, "Legislative and Quasi-Legislative Functions of ICAO: Towards Improved Efficiency" (1995) XX:I Ann. Air & Sp. L. 343 at 354.

[32] See *Chicago Convention*, *supra* note 23, art. 37 (j).

[33] See R.I.R. Abeyratne, "Facilitation and the ICAO Role – A Prologue for the Nineties" (1990) XV Ann. Air & Sp. L. 3 at 8.

of the scenario is often aggravated by the lack of collaborative spirit from the implicated participants.[34]

Annex 9 deals with Standards and Recommended Practices on Facilitation that have either: 1) a negative form, whereby States agree not to impose additional requirements, such as restrictions and paperwork; or 2) a positive form, whereby States agree to provide the minimum facilities needed for the proper circulation of passengers generated from air transport.[35] An International Standard, adopted by the Council pursuant to Article 54(l) of the Chicago Convention, obligates Contracting States to guarantee the highest practicable degree of adherence to its contents, and is necessary to facilitate and improve facets of international air navigation. In contrast, a Recommended Practice is a highly desirable guideline to be implemented by Contracting States to aid the progress of international air navigation.[36] The former uses the word "shall", indicating its mandatory applicability and the latter the word "should", giving a more flexible application.[37] Contracting States shall immediately notify the Council of non-compliance with a standard pursuant to Article 38 of the Chicago Convention.[38] Thus, as pointed out by R.I.R. Abeyratne: "the notification to the

---

[34] The original aims of ICAO in the field of Facilitation were:

> to achieve, to the maximum degree consistent with the public interest, free and unimpeded passage of aircraft and crews, passengers, baggage, cargo and mail that they carry on international flights. The principal means by which this aim can be accomplished are simplified and uniform procedures, amendments to regulations which may delay or restrict the movement of international traffic, and continuing efforts on the part for airport authorities and operators of international flights to reduce ground delays to a minimum.

ICAO, *Aims and Objectives of ICAO in the Field of Facilitation,* ICAO Doc. 7891-C/908, cited in B. Cheng, *Studies in International Space Law* (Oxford: Claredon Press, 1997) at 51.

[35] See Annex 9 (Facilitation) to the *Convention on the International Civil Aviation,* 10th ed. (April 1997) at (v) [hereinafter *Annex 9*].

[36] See ICAO, *Consolidated statement of ICAO continuing policies and associated practices related specifically to air navigation,* Assembly Resolution A32-14, app. A (October 1998).

[37] See R.I.R. Abeyratne, "The Role of Automation in Facilitation of Air Transport into the 21st Century" (1995) XX:I Ann. Air & Sp. L. 259 at 271.

[38] The Article reads as follows:

> Any State which finds it impracticable to comply in all respects with any such international standard or procedure, or to bring its own regulations or practices into full accord with any international standard or procedure after amendment of the latter, or which deems it necessary to adopt regulations or practices differing in any particular respect from those established by any international standard, shall give immediate notification to the International Civil Aviation Organisation of the differences between its own practice and that established by the international standard. In the case of amendments to international standards, any State which does not make the appropriate amendments to its own regulations or practices shall give notice to the Council within sixty days of the adoption of the amendment to the international standard, or indicate the action which it proposes to take. In any such case, the Council shall make immediate

Council does not absolve Contracting States from continuing securing the highest practical degree of uniformity".[39] Herein arises one of the main flaws of the ICAO system: a large number of Contracting States do not inform the Council of their current non-compliance with standards and procedures, thereby creating uncertainty and jeopardising air transport safety.[40] Legally speaking, Contracting States are not obliged to adopt standards and recommended practices, but are required to notify the Council of any difference from them.[41] Notwithstanding ICAO's magnificent law-making contribution to air navigation reached by the consensus of its members, assessing the worldwide degree of compliance with standards and procedures remains an extremely intricate task, which is far from being achieved, hence, severely overshadowing its accomplishments.

A comprehensive description of the contents of Annex 9 becomes mandatory to fully understand the efforts ICAO has undertaken to facilitate air traffic flows. An assessment of its significant achievements and flaws will also be covered. Consequently, Chapter 1 of Annex 9 establishes definitions and its scope, stressing applicability to all categories of aircraft operation, scheduled and non-scheduled, except where a particular provision states otherwise.

Chapter 2 covering entry and departure of aircraft, confers the "green light" to electronic data interchange (EDI) clearance of both passengers and cargo.[42] Accordingly,

---

> notification to all other states of the difference, which exists between one or more features of an international standard and the corresponding national practice of that State.

Ibid., art. 38.

[39] Abeyratne, *supra* note 19 at 268.

[40] See especially M. Milde, "The Chicago Convention - Are Major Amendments Necessary or Desirable 50 Year Later?" (1994) XIX:I Ann. Air & Sp. L. 401 at 425.

[41] See also ICAO, *supra* note 36, app. D.

[42] EDI has been regarded as "the electronic transfer, from computer to computer, of commercial and administrative data using an agreed standard to structure an EDI message". See EC, *Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange,* [1994] O.J. L. 338/98 at 102. See generally K.J. Kotch, "Addressing the Legal Problems of International Electronic Data Interchange: The Use of Computer Records as Evidence in Different Legal Systems" (1992) 6 Temple Int'l & Comp. L.J. 451; R. Drudmmond, "EDI and Internet" (1994) 4:2 EDI World 20; C. Reed, "EDI: Contractual and Liability Issues" (1989) 6 Computer L. 36; J.A. Smith, "Are Your EDI Transactions Safe? (A risk assessment methodology for EDI unclassified/sensitive information)" (1994) 5 CALS J. 76; R.V. Sabett, "International Harmonisation in Electronic Commerce and Electronic Data Interchange: A Proposed First Step Towards Signing in the Digital Dotted Line" (1998) 46 Am. L.R. 511; J.B. Ritter, "Current Issues in Electronic Data Interchange: Defining International Electronic Commerce" (1992) 13 J. Int'l L. Bus. 3; R.W. McKeon, Jr. "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" (1994) 12 J. Marshal J. Computer & Info. L. 511; A.H. Boss, "The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies" (1991) 46 Bus. Law. 1787; E. Clark, "The

Contracting States shall not require the presentation of the "General Declaration" and the "Passenger Manifest" when the information contained therein can be acquired in an alternative and acceptable manner.[43] Hence, the language of the provision supports the use of an alternative electronically equivalent technique. It is noteworthy that a complete abolishment of the passenger manifest and cargo manifest cannot be obtained, pursuant to their requirement established in the Chicago Convention.[44] *A priori*, the introduction of EDI methods could trigger the validity of computer-generated records as a question of evidence, which a large number of Contracting States may not yet be in a position to accept.[45] Moreover, insofar as practicable, Contracting States are urged not to interrupt the normal flow of passengers when complying with disinfecting requisites, which States may undertake in order to prevent the spread of diseases by means of air navigation in accordance with Article 14 of the Chicago Convention. In this regard, the adoption of regulations established by the World Health Organisation is vigorously suggested.

Notwithstanding the "cutting red tape spirit" of Annex 9, it makes a tenuous recommendation to Contracting States to adopt Memoranda of Understanding (MOU) with air carriers providing international services in order to contend with international trafficking of narcotics and pychotropic substances.[46] This crucial topic was only adopted as a "recommended practice", thus, *stricto sensu*, from a purely legal point of view its implementation can only be regarded as a highly desirable practice. This thesis supports replacing the aforesaid recommended practice with an "international standard" to strengthen the language of the provision. The importance of the subject merits a revision. Finally, Chapter 2 addresses the question of some arrangements concerning international general aviation and other non-scheduled flights.

Law of Electronic Commerce: EDI, Fax, and Email Technology, Proof, and Liability" (1992) 3:1 J.L. & Science 158.

[43] See *Annex* 9, *supra* note 35, standard 2.5.

[44] See *Chicago Convention*, *supra* note 23, art. 29 (f) & (g).

[45] The issue merits further study, which will be undertaken in chapter 3.

[46] See *Annex* 9, *supra* note 35, recommended practice 2.2.1. See also R.I.R. Abeyratne, "International Initiatives at Controlling the Illicit Transportation of Narcotic Drugs by Air" (1997) 63:2 J. of Air L. 289; R.I.R. Abeyratne, "Recent Measures Taken by ICAO and the United Nations to Control the Illicit Transportation of Narcotic Drugs by Air" (1998) 33:3 Eur. Transp. L. 321.

In tackling the issue of entry and departure of persons and their baggage, Chapter 3 strongly supports the use of Machine Readable Travel Documents (MRTD), *inter alia*, passports,[47] visas, crew member certificates, and the Advance Passenger Information System (API).[48] Moreover, Contracting States are vigorously encouraged to promote the internationally standardised formats for biometrics in travel documents to achieve a more accurate level of identity verification, thereby reducing the risk of fraud.[49] The language of this chapter goes even further, recommending that Contracting States extend to the maximum number of countries the practice of abolishing visa requirements through bilateral or multilateral arrangements.[50] The latter remains a highly desirable, yet unachieved practice, which realistically speaking, will never be fully accomplished on a global basis.[51] Furthermore, Chapter 3 tries to discourage Contracting States from requiring embarkation/disembarkation cards, which result in inconvenient delays for passengers and unnecessary, burdensome expenditures for airlines. Unfortunately, this ill-fated practice is still used by a large number of countries. Section IV deals with public health requisites compelling Contracting States to comply with the World Health Organisation regulations and practices. Finally, Chapter 3 talks about procedures for the inspection and control of persons, addressing the inspection of documents,[52] inadmissible persons,[53] deportees,[54] and the procurement of a replacement travel document[55] for the aforesaid cases.[56] This section of Annex 9 also seeks to include selective inspection target methods, the use of multiple-channel inspection procedures, and the "red and green" system for customs clearance of passengers.[57] The foregoing would remove low-risk passengers from the unnecessary torture they are currently exposed thereto.

---

[47] Annex 9 suggests to Contracting States that passports be rapidly expedited and valid for a period of at least five years, and that joint passports for two spouses be avoided. See *ibid.*, recommended practice 3.5.3, 3.5.4 & 3.5.8.
[48] MRTD & API will be thoroughly analysed in a following chapter.
[49] See *Annex* 9, *supra* note 35, recommended practice 3.5.10.
[50] See *ibid.*, recommended practice 3.7.
[51] The reasons are numerous and beyond the scope of this study; however, it is safe to mention immigration and distribution of economic wealth as some of the causes.
[52] See *Annex* 9, *supra* note 35, standard 3.39.
[53] See *ibid.*, standard 3.42.
[54] See *ibid.*, standard 3.52.
[55] See *ibid.*, standard 3.54.
[56] These issues will be examined in Chapter 3 when dealing with inadmissible passengers.
[57] See M. McMunn, "Aviation Security and Facilitation Programmes are Distinct but Closely Intertwined" (1996) 51:9 ICAO J. 7.

Chapter 4 deals with entry (import) and departure (export) of cargo[58] and other articles, and places particular emphasis on the introduction of electronic data-processing techniques for air cargo facilitation.[59] The language of the provisions seeks to persuade Contracting States, international airline operators, handling companies, airports, cargo agents, and other authorities to exchange data electronically following the recommendations and formats of the United Nations Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT).[60] These recommendations comprise a set of internationally agreed-upon standards, directories, and guidelines for the electronic interchange of structured data with particular emphasis on trade in goods and services between independent, computerised information systems.[61] A suggestion to implement the Guidelines for Expedited Clearance of the World Customs Organisation placed on the Contracting States stresses the co-ordinating spirit of the provisions thereof. Contracting States shall undertake efforts to release all general cargo requiring solely normal inspection within four hours from the time proper documentation or a legally acceptable electronic equivalent is presented.[62] Additionally, Chapter 4 sets the procedures for handling containers, pallets, and their loads;[63] it defines the limitation of operators' responsibilities;[64] it advocates eliminating customs duties for the importation of aircraft equipment, stores, and parts in accordance with Article 24 of the Chicago Convention;[65] and finally it speaks about cargo and other articles not entering the intended country of destination, such as unaccompanied baggage,[66] animal and plant shipments,[67] and mail documents.[68]

---

[58] Electronic documentation is considerably manifesting in air cargo operations as the normal *modus operandi*. See J. Musselwhite, "Air Cargo Information Systems" *Aviation Informatics* (October 1995) 4.

[59] In the private sector, the air transport industry has seen the emerging role IATA has played with respect to the facilitation of air cargo. IATA's endeavours include, *inter alia*, establishing cargo release and entry/clearance procedures, and encouraging the transmission of information electronically (EDI). Through resolution 606, IATA has set the standards for cargo bar coding. See IATA, "Cargo Facilitation" online: Http://www.iata.org/cargo/facilitation.html (date accessed: 30 June 2000) See also J. Gallacher, "Cargo chasing the value chain" *Airline Business* (November 1998) 52; IATA, "IATA and Cargo EDI" Online: Http://www.iata.org/cargo/edi.html (date accessed 17 May 2000); F. Philipson, "Yields making cargo pay" *Airline Business* (November 1998) 64; P. Conway, Peter, "Cargo on-line" *Airline Business* (February 2000) 76; M. Odell, "Freight Frighteners" *Airline Business* (March 1997) 60.

[60] See United Nations Economic Commission for Europe, "UN/EDIFACT Draft Directory" online: http://www.unece.org/trade/untdid/texts/d100_d.html (date accessed: 21 June 2000).

[61] See *Annex 9*, *supra* note 35, standard 4.41.

[62] See *ibid.*, recommended practice 4.29.1.

[63] See *ibid.*, standard 4.35.

[64] See *ibid.*, standard 4.41.

[65] See *Chicago Convention*, *supra* note 23, art. 24(b). See also *Annex 9*, *ibid.*, recommended practice 4.46.

[66] See *Annex 9*, *ibid.*, standard 4.57.

[67] See *ibid.*, standard 4.58.

[68] See *ibid.*, standard 4.59.

In one of the most overlooked parts of Annex 9, Chapter 5, focuses on traffic passing through the territory of a Contracting State and attempts to eliminate examination of crews, passengers, baggage, cargo, and mail whose final destination is another international port of entry.[69] Similarly, this chapter contains an international standard aimed at abolishing the requirement of in-transit visas; however, national authorities can circumvent it by claiming special circumstances and public interest.[70] Although one can understand the necessity of certain States requiring in-transit visas for "special circumstances", it has also constituted a discretionary shield where some States shelter their greedy desire of generating extra income, leading to the formation of unnecessary hurdles that slow the flow of air passengers considerably. Likewise, Chapter 5 seeks to expedite the transfer of in-transit passengers having a connecting flight at the same airport;[71] or at another airport.[72] It also suggests the arrangement of the formalities of intermodality cargo traffic being transferred between air and surface transport,[73] and finally it encourages Contracting States to develop free airports and free zones in accordance with Article 23 of the Chicago Convention.[74] The *rationale* of the provision attempts to facilitate the movement of air traffic at connecting points by abolishing formalities to the maximum extent feasible, which has been shown to be of paramount significance in developing so-called "hub airports". Paradoxically, there are still a large number of airport terminals in rather large cities, such as Buenos Aires in Argentina, where these standards have not even been partially implemented.[75]

In addition to encouraging the exchange of all relevant flight information by EDI in accordance with UN/EDIFACT,[76] Chapter 6 advocates ensuring *de rigueur* facilities and services, which are essential for the rapid handling and clearance of passengers, crews, baggage, cargo, and mail. Taking into account the previously mentioned statistics on significant, rapid air traffic growth, suitable management of adequate infrastructure remains

---

[69] See *ibid.*, standard 5.1.
[70] See *ibid.*, standard 5.2.
[71] See *ibid.*, standard 5.3.
[72] See *ibid.*, standard 5.8.
[73] See *ibid.*, standard 5.10.
[74] See *ibid.*, recommended practice 5.11.
[75] Argentina has yet to file a difference with ICAO in this respect. See ICAO, *Supplemental edition to Annex 9*, forthcoming in November 2000.
[76] See *Annex 9, supra* note 35, recommended practice 6.7.1

indispensable.[77] Passenger services charges should be levied by the airlines in ways that steer clear of lengthy queues at international airports.[78] Additionally, the use of credit cards should be acceptable as a means of payment for the aforesaid charges.[79] Absurdly enough, at Montreal's Dorval International Airport the so-called "Airport Improvement Fee", which is not regarded as a tax, is indeed collected by airport personnel, resulting in excessive queues and delays that are contrary to ICAO's recommended practices.[80] Hence, this thesis supports a broader concept of "service charges", including other types of airport-related taxes, duties, and fees charged to passengers, envisaging their collection by the airline, who will then return those funds to the taxing authority. Doing so, would simplify airport procedures for passengers, cargo, and mail departure considerably.

One major ICAO objective is to accomplish through its facilitation programme the completion of all departure formalities within 60 minutes for all passengers requiring no more than normal inspection on international air transport services, calculated from the time the passenger presents himself at the first processing point at the airport.[81] For incoming passengers, ICAO targets a 45-minute disembarking clearance, regardless of aircraft size or arrival time.[82]

Ideally, Contracting States should provide, *inter alia*, facilities and services for public health,[83] emergency medical relief, animal and plant quarantine,[84] child care,[85] storage,[86] physical transit and transfer areas for passengers and crews,[87] monetary exchange,[88] clearance controls and operation of control services,[89] and cargo and mail handling clearance.[90] However, the difference in terms of economic capabilities of Contracting States reflects

---

[77] See *ibid.*, standard 6.1.
[78] See *ibid.*, recommended practice 6.4.
[79] See *ibid.*, recommended practice 6.5.
[80] Canada has yet to file a difference with ICAO in this respect. See ICAO, *supra* note 75.
[81] See *Annex* 9, *supra* note 35, recommended practice 6.16.
[82] IATA is trying to conclude agreements with different governments, ensuring that all possible formalities are abolished to comply with the 45-minute arrival clearance timeframe. See M. Momberger, "Speeding Up Air Travel on the Ground" *Airport Forum* XXV:3 (June 1995) 32.
[83] See *Annex 9*, *supra* note 35, recommended practice 6.54.
[84] See *ibid.*, recommended practice 6.55.
[85] See *ibid.*, recommended practice 6.18.
[86] See *ibid.*, recommended practice 6.37.1.
[87] See *ibid.*, recommended practice 6.35.
[88] See *ibid.*, recommended practice 6.65.
[89] See *ibid.*, recommended practice 6.60.
[90] See *ibid.*, recommended practice 6.40.

another scenario, especially in developing countries where there is sometimes the will to comply with standards, procedures, and suggestions, but where a lack of financial means prevents the achievements of these significant recommendations.

Addressing the issue of aircraft landing in other places than at international airports, Chapter 7 aims at commanding Contracting States to ensure that all possible assistance and applicable procedures have been rendered to an aircraft that for reasons beyond the pilot-in-command has landed elsewhere.[91] Chapter 8 addresses other facilitation provisions, such as bonds and exemption from requisition or seizure,[92] facilitation of search, rescue, accident investigation and salvage,[93] relief flights following natural and man-made disasters,[94] marine pollution and safety emergency operations,[95] facilitation of the transport of passengers requiring special assistance,[96] and last but not least, the implementation of national facilitation programmes.[97] These programmes promote the removal of obstacles and delays in the movement of aircraft, crews, passengers, cargo, mail, and stores. In addition, Chapter 8 foresees the creation of a National Air Transport Facilitation Committee and an Airport Facilitation Committee for purpose of co-ordinating facilitation activities, projects, and objectives.[98] The gathering of participant must include, but not be limited to, *inter alia*, air carrier operators (including forwarders and express carriers), civil aviation authorities, airport authorities, government clearance agencies (including customs, immigration, consular, passport and visa, public health, agriculture, security and narcotics control), and other government agencies not directly related to air transport (as is the case of postal services,

---

[91] See *ibid.*, standard 7.1.
[92] See *ibid.*, recommended practice 8.1.
[93] See *ibid.*, standard 8.3. See generally ICAO, *Co-ordination of activities between the United Nations and ICAO relating to emergency action to assist in the maintenance of international peace and security*, Assembly Resolution A5-5, online: http://www.icao.int/icao/en/res/a5_5.html (date accessed: 23 August 2000).
[94] See *ibid.*, standard 8.8. See generally R.I.R. Abeyratne, "Relief Flights and Humanitarian Intervention: Perspectives in International Law" (1995) 44:1 Z.L.W. 3.
[94] See *Annex 9*, *ibid.*, recommended practice 8.1.
[95] See *ibid.*, standard 8.10.
[96] See *ibid.*, recommended practice 8.22. See also ICAO, News Release PIO 4/95, "ICAO Facilitation Meeting Considers Aircraft Disinsection, Public Health, Asylum Seekers and Persons with Disabilities" (April 1995), online: http://www.icao.int/icao/en/nr/pio9504.html (date accessed: 9 July 2000). See generally R.I.R. Abeyratne, "Proposals and Guidelines for the Carriage of Elderly and Disabled Persons by Air" (1995) 33:3 J. of Travel Research 52.
[97] See *Annex 9*, *ibid.*, standard 8.17.
[98] See *ibid.*, standard 8.19.

tourism, and trade departments).[99] The full implementation of the national facilitation programme seems to be the best legal vehicle for players to propose their initiatives, make inquiries, and formulate suggestions to ultimately achieve the desired ease in the flow of air traffic components. The Annex also provides a set of models for establishing national facilitation programmes under Appendix 11.[100]

Hitherto, this thesis has analysed the legal framework created by the Chicago Convention and Annex 9 with respect to facilitation; however, two of the major risks that implementing the provisions contained in those instruments deal with, drug trafficking and security, will be examined hereafter.

1.3. Conflict of Interests - Facilitation *vis-à-vis* Drug Trafficking and Security

By streamlining immigration lines and simplifying customs clearance procedures, both of which enhance the flow of air traffic, Contracting States run the unaffordable risk of hindering international civil aviation security as well as lessening drug trafficking control measures.[101] Then, an unavoidable and irreconcilable conflict of interests unmistakably materialises.

The Chicago Convention does not *prima facie* tackle the illicit transportation of narcotic drugs directly; *a posteriori*, a careful assessment identifies that various provisions do stand out, essentially emphasising the surveillance *potestas* bestowed upon States for aircraft, crews, passengers, cargo, and mail.[102] Similarly, the Chicago Convention attempts to ban any possible "misuse" of civil aviation through Article 4, even though the word "misuse" is only

---

[99] See *ibid.*, app. 12.

[100] As a matter of fact, Paraguay has included in the proposed Aeronautics Code the structure for implementing the national facilitation committee. Bill 454 has yet to be passed by Congress.

[101] Michael Milde has noted the significant number of seizures of narcotic drugs and psychotropic substances at international airports particularly transported in general aviation. However, he stresses that the scenario in commercial aviation is not exceptionally promising either, since "66.5 per cent of the narcotics seized in commercial aviation were hidden in the luggage of passengers; 21.1 per cent were concealed on the person of the passenger, 9.2 per cent were internally concealed and 1.2 per cent were concealed in the air frames and other locations accessible only to the carriers' personnel". M. Milde, "The Role of ICAO in the Suppression of Drug Abuse and Illicit Trafficking" (1988) XIII Ann. Air & Sp. L. 133 at 147-148, citing *The Drug Problem*, ICAO Doc. AN-WP/5918.

[102] See *Chicago Convention*, *supra* note 23, arts. 10, 13, 16 & 35.

included in the heading of the text and not in its substance.[103] Although a first reading of the article would seem to connote that any feasible use of civil aviation contrary to the purposes of the Chicago Convention is forbidden, a further analysis will show this is not so. Milde has mentioned that "Article 4 is of no relevance to the problem of criminal use of civil aviation (such as drug trafficking) since it refers only to the obligations of Sates and to the acts of States."[104] Similarly, Abeyratne has mentioned that Article 4 is inapplicable because it has never been dealt with by the Assembly or Council, and that according to its drafting history the purpose thereof was to prevent States from imperilling other States by misusing civil aviation.[105] Furthermore, no provision in the Chicago Convention directly addresses the issue of drug trafficking, *a fortiori*, ICAO has recognised the necessity of adopting severe measures to prevent the illicit transport of narcotic drugs and psychotropic substances.[106] As mentioned in the preceding section, those provisions dealing with drug trafficking in Annex 9 are only "Recommended Practices", which reflects to what degree Contracting States were willing to compromise on this matter. However, one effective way to counterattack the rise in drug trafficking in air transport without contradicting the spirit of Annex 9 would be to implement random checks of aircraft, baggage, and cargo. Such sporadic, selective checks could primarily target high-risk passengers, hence, not slowing the flow of passengers.[107] Needless to say that the complexity of the drug trafficking problem calls for an interactive gathering of efforts amongst the various participants attempting to progressively diminish drug trafficking in air transport.[108]

---

[103] The text reads: "Each contracting State agrees not to use civil aviation for any purpose inconsistent with the aims of the Convention."

[104] See M. Milde, "Interception of Civil Aircraft vs. Misuse of Civil Aviation" (1986) XI Ann. Air & Sp. L. 105 at 122.

[105] See R.I.R. Abeyratne, "International Initiatives at Controlling the Illicit Transportation of Narcotic Drugs by Air" (1997) 63:1 J. of Air L. 289 at 397. The original purpose of the article was to reduce the possibility of threatening acts to States by the use of civil aviation. Article 4 originated in the Canadian "Preliminary Draft" of the Chicago Convention, which was based on the text of the Treaty for the Renunciation of War of 27 August 1928, known as Briand-Kellog Pact. See Milde, *supra* note 104 at 123.

[106] See ICAO, *Role of ICAO in the suppression of illicit transport of narcotic drugs by air*, Assembly Resolution A27/12 (October 1989), online: http://www.icao.int/icao/en/res/a27_12.html (date accessed: 15 August 2000). See generally *Declaration of the International Conference on Drug Abuse and Illicit Trafficking and Comprehensive Multidisciplinary Outline of Future Activities in Drug Abuse Control*, U.N. Doc. StT/NAR/14, U.N. Sales No. E.88 XI (1988).

[107] See Milde, *supra* note 101 at 151. However, one can question the effectiveness of random checks in preventing the transport of illicit narcotic drugs for the remaining non-inspected part of the traffic.

[108] See R.I.R. Abeyratne, "Recent Measures Taken by ICAO and the United Nations to Control the Illicit Transportation of Narcotic Drugs by Air" (1998) XXXIII Eur. Transp. L. 321 at 344.

to approach the dilemma with the necessary balance, ICAO has merged the administration of its security and facilitation programmes.[113]

Although the foregoing initiatives are to some extent extremely valuable to strengthen security and fortify drug trafficking control in civil aviation, one could reasonably question the validity of those legal provisions, which in practical terms are not enforceable when non-compliance situations arise.[114] The latter must become a mandatory concern of all participants involved in civil aviation, where compromises should be made in order to guarantee the longed-for equilibrium between taking risks and achieving critical objectives, which will ultimately contribute to setting up the necessary path for cutting red tape in air transport.

---

[113] See McMunn, *supra* note 57.

[114] Although beyond the scope of this thesis, one way by which ICAO checks the compliance of Contracting States with the provisions contained in the Annexes has been the assessment of Safety Oversight Audits amongst its members, but covering only provisions contained in Annexes 1, 6 & 8. Audits are primarily concerned with safety issues, and are only conducted with the approval of the audited Contracting State. It is reasonable to foresee that the provisions contained in Annex 9 will be the last to form part of ICAO's oversight audit programme. See also ICAO, *Establishment of an ICAO universal safety oversight audit programme*, Assembly Resolution A32-11 (1998), online: http://www.icao.int/icao/en/res/a32_11.html (date accessed: 24 August 2000). See generally S. Manning, "The United States' Response to International Air Safety" (1195-1996) 61 J. of Air L. 505 at 511; G.N. Tompkins, Jr., "Enforcement of Aviation Safety Standards" (1995) XX:I Ann. Air & Sp. L 319; R.D. van Dam, "Recent Developments in Aviation Safety Oversight" (1995) XX:I Ann. Air & Sp. L. 307.

Chapter two

Cutting Red Tape

Smoothness in the flow of air transport is a mandatory concern if the players want to cope with the increasing demand of traffic and the industry's adequate responses thereto. Consequently, one of the major focuses of the implementation of automation in facilitation of air transport relies on customs and immigration clearance procedures, which remain extremely formalistic and bureaucratic. As a matter of fact, a recent survey conducted by American Express revealed that 31% of the passengers interviewed ranked the slowness of security clearance and passport control as what they hated most about airline services.[115] Another report has showed that the more free time passengers possess after completing all required formalities, the more time they have to spend money on the surrounding infrastructure, which will eventually lead to a considerable swelling in airport concession revenues.[116] This creates an incentive for the industry players to gather initiatives, endeavours, and efforts in order to create the necessary automation environment in air transport.

The foregoing explanation sustains the significance of achieving the longed-for "cutting red tape" goals to ultimately achieve a hassle-free environment for air transport passengers. Accordingly, this thesis will proceed to thoroughly analyse certain endeavours undertaken by a conglomerate of vital industry players aiming to clear the way to accomplish such goals.

2.1. Machine Readable Travel Documents

Pursuant to the mandate bestowed by Article 37 of the Chicago Convention, ICAO, through its Facilitation Division, has been particularly keen on developing international standards and recommended practices for customs and immigration procedures through the implementation of studies on travel documents. Besides facilitating the flow of passengers through numerous formalities, these projects have ultimately been aimed at obtaining from Contracting States the waiver of passport and visas, accepting "travel cards", "non-

[115] See R. Bond & D. Guillebeaud, "Surviving the Customer" *Airline Business* (March 1997) 54.

immigrant cards" or "international passenger cards" in lieu thereof.[117] Needless to say, this objective remains somewhat unattainable on a global basis, particularly considering the varied distribution of wealth globally and its remarkable consequences on immigration, problems that create a myriad of issues considerably difficult to manage, even for powerful countries such as the United States.[118]

2.1.1. Machine Readable Passports

Consequently, ICAO has set its goals according to what is indeed feasible. Thus, by focusing on developing mechanisms to accelerate passport control clearance, ICAO elaborated the idea of a Machine Readable Passport (MRP). Legally speaking, a passport *per se* is an official document capable of having legal consequences that denotes the identity and nationality of a person, thereby assuring to the State of destination that the bearer is eligible for return to the State that issued the passport.[119]

Conceived with a dual function, an MRP possesses a machine-readable zone, enabling a rather rapid machine clearance, quick verification, and immediate recording of the personal data contained therein.[120] Ideally at the passport control unit, the agent places the passport face down and swipes it through the scanning device; the data is then automatically transmitted to the authority's computer system. Additionally, an MRP also encompasses a descriptive, visual zone with all the data of the passport holder in case the passport control

---

[116] See "Beating ICAO Passenger Processing Times" *Airport World* 3:3 (June-July 1998).
[117] See R.I.R. Abeyratne, "The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject" (1992) XVII:II Ann. Air & Sp. L. 1 at 2.
[118] For an interesting comment on immigrations problems related to air transport, see generally C. O'Keefe, "Immigration Issues and Airlines: An Update" (1997) 63:1 J. of Air L. 17; E.G. Yost, "Immigration and Nationality Law" (1997) 31 Int'l Lawyer 589; P. Tompkins, "Immigration Controls at International Airports in the 21st Century" *Aviation Security International* 3:6 (March 1994); R. Bray, "Immigration Taking Smart Steps" *Financial Times* XI (4 September 1997); A. McCallen, "Non-Immigration Visa Fraud: Proposals to End the Misuse of the L Visa by Transnational Criminal Organisations as a Method of Illegal Immigration" (1999) 32 Vand. J. Transnat'l L. 237. For an interesting study on immigration problems faced by developed countries, see generally Organisation for Economic Co-operation and Development, *Trends in International Migration* (Paris: OECD, 1999). For a comprehensive assessment of immigration and its economic impact on communities in the United States see B. Baker-Kelly, "United States Immigration: A Wake Up Call!" (1994) 37 How. L.J. 283 at 287-288.
[119] See ICAO, *International co-operation in protecting the security and integrity of passports*, Assembly Resolution A32-18 (1998), online: http://www.icao.int/icao/en/res/a32_18.html (date accessed: 26 June 2000).
[120] See Abeyratne, *supra* note 117 at 6.

authorities do not have the scanning machines or the proper software to fully undergo clearance with an MRP.

ICAO published the first specifications and guidelines on the construction of MRPs in 1980, especially clarifying the sections of the documents containing details of the holder.[121] Subsequently, the Technical Advisory Group on Machine Readable Travel Passports (TAG-MRTP) was established in 1984. A year later, the International Standard Organisation (ISO) adopted those specifications and guidelines.[122] Nevertheless, understanding that it is not yet feasible to achieve worldwide use of MRPs, ICAO has only recommended their use in Doc. 9303,[123] as opposed to imposing a more stringent implementation through an international standard. ICAO has strongly suggested that Contracting States standardise the personal identification data included in their passports with the specifications and guidelines enclosed in ICAO Doc. 9303, even when they are not machine readable.[124]

2.1.2. Machine Readable Visas

In 1991, ICAO renamed the Technical Advisory Group on Machine Readable Passports (TAG/MRP) the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), expanding its scope to include the development of guidelines and specifications for Machine Readable Visas (MRV).[125] Undoubtedly, ICAO hopes to eliminate the requirement of visas as much as possible;[126] however, since numerous Contracting States may still require the presentation of visas, ICAO has recommended their adoption in a machine-readable form.[127] Although only a small number of countries have successfully experimented with implementing machine-readable visas, the results have been

---

[121] See ICAO, *Machine Readable Passport*, ICAO Doc. 9303 Part 1, 1st ed. (1980). However, ICAO has already published the fourth edition on machine readable passport, see ICAO, *Machine Readable Passport*, ICAO Doc. 9303 Part 1, 4th ed. (1999).
[122] See ISO, *Identification Cards – Machine Readable Travel Documents – Part 1: Machine Readable Passport*, Doc. 7501, 3rd ed. (1997).
[123] See *Annex 9*, *supra* note 35, recommended practice 3.5.1.
[124] See *ibid.*, standard 3.4.1.
[125] Like MRPs, MRVs contain both a machine-readable zone and a visual zone; the scanning data process is also the same as for MRPs.
[126] See *Annex 9*, *supra* note 35, recommended practice 3.7.
[127] See *ibid.*, recommended practice 3.8.1.

quite positive, considering the capability of a rather instantaneous clearance of visitors.[128] In 1997, ICAO Doc. 9303 Part 2 received international certification from the ISO.[129]

2.1.3. Machine Readable Official Travel Documents

Subsequently, with the advent of globalisation and regional markets such as the European Union, leading to the emerging use of various forms of official identity documents for travel purposes, *inter alia*, US resident alien cards, Latin American identity cards, and electronic European identity and travel documents, ICAO has determined the need for generic specifications for two sizes of machine-readable official travel documents, referred to as TD-1s and TD-2s respectively.[130] TD-1 foresees a card of 54.0 mm x 85.6 mm (2.13 in x 3.337 in), and TD-2 a card of 74.0 mm x 105.0 mm (2.91 in x 4.13 in), in accordance with ISO 7810.[131] Through these generic specifications, ICAO intends to harmonise international standards for liberal States wishing to accept other types of identification as valid travel documents.[132]

2.1.4. Machine Readable Crew Member Certificates

Within the same trend, ICAO has established guidelines and specifications for the creation and respective layout of machine-readable crew member certificates, which might be used for travel purposes by air crew members (both flight crews and cabin attendants) in lieu of passports or visas, leaving crew licences to serve their primary purpose, to attest to crew members professional qualifications.[133]

Unarguably the use of MRTDs have a myriad of advantages, *inter alia*, the enhancement of security, avoiding to a certain extent travel documents counterfeiting,

---

[128] See ICAO, *Machine Readable Travel Documents - Machine Readable Visas*, ICAO Doc. 9303 Part 2, 2nd ed. (1994).
[129] See ISO, *Identification Cards - Machine Readable Travel Documents - Part 2: Machine Readable Visa*, Doc. 7501-2, 2nd ed. (1997).
[130] See ICAO, *Machine Readable Travel Documents - Size 1 and Size 2 Machine Readable Official Travel Documents*, ICAO Doc. 9303 Part 3, 1st ed. (1996).
[131] See ISO, *Identification Cards – Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents*, ISO 7501-3 1st ed. (1997).
[132] See *Annex 9*, *supra* note 35, standard 3.4.
[133] See *ibid.*, recommended practice 3.23.1.

forgery, and alteration,[134] the almost instantaneous verification and recording of data, the smooth immigration clearance of low-risk passengers, the elimination of landing forms, and the ability to handle increased airport capacity.[135] Notwithstanding the grandiloquent ICAO achievement with respect to MRTDs in terms of creating the necessary specifications and guidelines to harmonise international standards, there still remain a large number of countries not in a position to follow these "automation trends". Until a global degree of uniformity is achieved, there is still territory for the Facilitation Section of ICAO to conquer.[136]

2.2. Advance Passenger Information (API)

The Chicago Convention enunciates that every aircraft engaged in international navigation transporting passengers shall carry a list with their names and place of embarkation and destination.[137] Hence, bearing in mind the aforesaid international obligation, but aiming at simplifying formalities, ICAO has been in favour of eliminating as much paperwork as possible in this respect. One way of accomplishing such goal is by transmitting such data by means of EDI, which was contemplated in the last revision of Annex 9.[138]

Originally a US Customs programme, the API has been designed to expedite the processing of passengers arriving in the United States, enhancing the control of such threats such as national security and drug trafficking.[139] At passenger check-in, airline operators input the passenger information into their computer system as enclosed in the machine- readable zone of the passport. Then, while the aircraft is still in flight, the information is sent to the

---

[134] Nevertheless, MRTPs are by no means immune to those risks. Concerns about the security and integrity of passports have been expressed at ICAO. See ICAO, *supra* note 119. See generally J. Nicol, "Passports for Sale" *Maclean's* (3 April 2000) 16.

[135] Another significant accomplishment in developing MRTDs has been the standardisation of the use of different alphabets worldwide, and the limitation to a certain number of characters for extremely long names.

[136] Although there are currently no official figures on compliance with the MRTDs recommendations, unofficially ICAO believes that around 109 Contracting States have issued or are planning to issue MRPs in accordance with the technical specifications of Doc. 9303 Part 1; 24 Contracting States have issued MRVs and 6 have issued crew member certificates.

[137] See *Chicago Convention, supra* note 23, art. 29.

[138] See *Annex 9, supra* note 35, standard 2.5.

[139] On 1 April 1998, Customs, the Immigration and Naturalisation Service (INS), the Animal Plant Health Inspection Service (APHIS), and 39 air carriers concluded a Memorandum of Understanding (MOU) to establish a written set of data quality standards for the Advance Passenger Information System (APIS). See US Customs, "Advance Passenger System" online: http://www.customs.gov/impoexpo/tools/archives/vol2n01/moujul.html#top (date accessed: 23 June 2000).

centralised Customs System Unit for verification against inter-agency databases and lookout lists. The results are distributed to Immigration and Customs prior to the arrival of the flight. Once the passenger presents himself at the Passport Control Unit, through the so-called expedited ABlue line, the passport is scanned through API reader devices to verify the data originally input. API Systems remarkably reduce time, eliminate queues, confer examining authorities with extra time, and grant the airline passenger a specific expedited "premium service" immigration clearance line, thereby smoothing traffic flows.[140] Hence, ICAO has been in favour of recommending that its Contracting States implement API Systems and that in doing so they join the World Customs Organisation (WCO)/IATA Guidelines on API.[141] Although they have numerous benefits, API Systems are still quite onerous if one considers the computer software, hardware, and the training of the personnel involved; this makes its worldwide use and acceptance far from being completely accomplished.[142]

Another major step towards automation of customs red tape has been the announcement of the Department of Treasury of the US Customs Service with respect to a programme test for the transfer of accompanied international in-transit baggage, which refers to baggage arriving in the United States aboard one aircraft and departing from the United States aboard another.[143] For purposes of US regulations, accompanied international in-transit baggage is deemed as cargo. According to the US Customs Regulations,[144] air carriers arriving in the United States are required to file an air cargo manifest for all cargo on board; this can be done either manually or by an electronic manifest under the Automated Manifest System (AMS).[145] Under this test programme the participant air carrier would transmit the data electronically via the API System prior the flight's arrival, as opposed to filing a cargo manifest for the in-transit baggage.

---

[140] See ICAO, "Facilitation, Advance Passenger Information" online: Http://www.icao.org/ico.en/atb/fal/api.html (date accessed: 22 June 2000).

[141] See *Annex 9*, *supra* note 35, recommended practice 3.14.2.

[142] As of 23 June 2000, 66 air carriers have signed the Advance Passenger System MOU, tantamount to 78% of all non pre-cleared international passengers. See US Customs, "U.S. Customs Service Goals for the Year 2000 – High Impact Agency Initiative" online: http://www.customs.gov/about/hi-impact.html (date accessed: 23 June 2000).

[143] Department of the Treasure, US Customs Service, "Announcement of a General Program Test: Procedure for Transfer of Accompanied (International) In-transit Baggage" online: http://www.customs.gov/new/fed-reg/notices/914538.html (date accessed: 23 June 2000).

[144] See 19 C.F.R. § 122.48 (a). This requirement directly contradicts the spirit of *Annex 9*, *supra* note 35, c. 5, recommended practices 5.1,5.3, & 5.5.

The legal relationship between the US Government and air carriers is established through the signing of a Memorandum of Understanding (MOU), which "outlines mutual goals for improving passenger processing".[146] Despite the mutual interest in achieving such goals, one can rightly question the degree of enforceability of an MOU, which is indeed a gentlemen's accord *per se*; but not yet a binding contract.[147] Should the air carrier not comply with the data quality performance standards established therein, the US Government simply reserves the right to cancel its inclusion in the API programme. The MOU represents somewhat of a gathering of efforts but with no real legal compromise.

The processing of passenger data through EDI[148] in the API System tackles several other legal matters of supreme significance, particularly for third parties. The first one, although not purely legal, is concerned with the security of the information handled therein, avoiding any possible intrusion causing alteration, destruction, or data loss thereof. The idea is to provide an "end-to-end" secure environment where trading partners can normally perform their business transactions.[149] It is reasonable to assume that the MOU in question will contain provisions addressing the parties' interests in ensuring the integrity and due care of data processed. This would reflect the necessity for adequate technological system infrastructure in order to grant the mandatory information confidentiality thereof.[150] Most

---

[145] See 19 U.S. C. 1431.

[146] See US Customs, *supra* note142.

[147] An MOU is equivalent to a "letter of intent", which in common law contract means a preliminary, non-committal understanding of the parties, who do not intend to be bound thereby but who may later plan to enter into a contract or another source of agreement. See *Black's Law Dictionary,* 7th ed. (St. Paul, Minnesota: West, 1999) at 916 & 998. The jurisprudence and doctrine have been rather cautious when defining and assessing the degree of enforceability of letters of intent. However, there is a general belief that in most cases when the parties opt for a letter of intent, such as the MOU, they do not intend to be bound by it or to comprise themselves thereto. See M. Furmston, K. Gakuin & J. Poole, *Contract Formation and Letters of Intent* (Chichester, England: John Wiley & Sons, 1998) at 144; E.A. Farnsworth, *Farnsworth on Contracts,* 2nd ed., vol. 1 (New York: Aspen Law & Business, 1998) at 214; R.B. Lake & U. Draetta, *Letter of Intent and Other Precontractual Documents* (Stoneham, Massachusetts: Butterworth Legal Publishers, 1989) at 21.

[148] The European Commission has made some legal recommendations with respect to EDI. The recommendation was supposed to remove uncertainty arising from the use of EDI. Hence, the Commission created a Model European Legal EDI Agreement, which comprises a set of model provisions. See EC, *Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange,* [1994] O.J. L. 338/98 at 110.

[149] J. Sherwood, "EDI Security" in B. Welch, ed., *Electronic Banking and Security*, (Cambridge, Massachusetts: Blackwell Publishers, 1994) at 164.

[150] The European Community, expressing some concerns about the security of information systems, has recommended a comprehensive revision of their vulnerability, and an assessment of the risk of breaches

likely the parties will mutually agree not to disclose or transmit the data to any unauthorised persons, nor to use the information for any purposes other than those originally intended by the parties. Secondly, using EDI creates an overt concern regarding the inexorable question of privacy. Although this particular legal issue will be comprehensively analysed hereafter, one can safely question to what extent a non-binding, non-committal, non-enforceable MOU can guarantee adequate data privacy protection of individuals, the third parties thereto, who ultimately could be affected by privacy infringements causing damages to them.[151] Thirdly, the transmission of data from country to country triggers the applicability of transfer of data protection laws, which may substantially differ among different nations. This issue will be also covered in the section addressing the legal implications of implementing these new industry trends.

2.3. Smart Cards

American Ted Hoff succeeded in creating the chip in 1971, but it wasn't until Frenchman Roland Moreno obtained a patent for the computer chip in 1974 that the idea of embedding one into a card really took off.[152] Primarily influenced by the need to overcome inadequate telecommunication conditions, the original development of smart cards appeared predominately in France as a tentative response to the aforesaid inconveniences with particular applications for telephone and banking cards.[153] The scenario in the United States was quite different. The telecommunication infrastructure was quite superior; hence, there was no need to develop a new system, which explains its rather later expansion *vis-à-vis* France.

Albeit the size of a credit card, a "Smart Card" possesses an integrated circuit chip through which information is processed. The chip enables the card to have computer capabilities, *inter alia*, memory, intelligence, logic, and processing power. In comparison with

---

thereof. See EC, *Council Decision of 31 March 1992 in the field of security of information systems*, [1992] O.J. L.123/19 at 23.

[151] Although beyond the scope of this thesis, the non-enforceable MOU also raises the question of the signatories' legal responsibility and liability in cases of misuse of personal data that may eventually cause damages to third parties.

[152] See C. Allen & J. Kutler, "Overview of Smart Cards and the Industry" in C. Allen & W.J. Bar, eds., *Smart Cards* (New York: McGraw-Hill, 1997) 2 at 3.

[153] *Ibid.*

the long-used magnetic stripe, a chip embedded in a smart card upgrades the card's security feature, enlarges storage data capacity, and lessens the probability of the card being damaged. There are two types: 1) "Intelligent Smart Cards", which, through a central processing unit, secure and store information, and make decisions based on specifications dictated by the card's issuer; and 2) "Store Value Memory Cards", which store pre-paid values that are deducted as the card is used (e.g., telephone cards, transportation cards of certain cities, such as Washington, DC and San Francisco in the United States).[154] If stolen or misplaced, anyone can use it, since it only requires a proper reader device.

Smart cards could have applications in such fields as telecommunications, banking, transport, travel and entertainment, health care, and national identification. Notwithstanding the numerous advantages, the implementation of smart cards still remains extremely difficult, particularly due to the extraordinary outlay of money needed to establish the system. Therefore, the development of multi-functional smart cards, serving as combined instruments of payments, providing access to loyalty programmes, and performing functions of identity cards and travel documents, has been foreseen with the foremost objective of gathering diverse players, thereby reducing the ultimate cost of the product.[155] Another major drawback in implementing smart cards is customers' fear of privacy intrusion. Indeed, a survey undertaken by the Smart Card Forum in 1994 revealed that 75% of the people interviewed considered that smart cards do not guarantee the privacy of the data contained therein.[156] Consequently, perhaps one of the most overlooked aspects in creating a smart card environment is building up customer trust thereof.[157] Although of minimal concern, another sensitive issue when dealing with smart cards is the possibility of counterfeit, forged, and false cards, a risk that could be substantially eliminated by introducing "Biometric" measurements thereto. Biometrics, a cutting-edge technology, would tremendously

---

[154] See C. Allen & J. Kutler, *supra* note 152 at 4. See also IATA, "Smart Card Technology" online; http://www.iata.org/smartcard/news.html (date accessed: 23 June 2000); J. Stillwell, "Will Smart Cards Take Flight?" *Aviation Informatics* (November 1996) 25 at 26.

[155] See B. Vis, "The Importance of Smart Cards" *Airport World* 3 (15 June 1996) 25 at 27. See generally R.R. Jueneman & R.J. Robertson, Jr., "Biometrics and Digital Signatures in Electronic Commerce" (1998) 38 Jurimetrics J. 427 at 452-453.

[156] See W. Keenan, M. Rea & G. Hubbard, "Components of the Business Proposition" in C. Allen & W.J. Barr, eds., *Smart Cards* (New York: McGraw-Hill, 1997) 21 at 30. See also A. de Groot, "Social Risk of Chipcards" in F. Knopjes & P.J. Lakeman, eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999) 69.

[157] For an interesting study on the public trust in the use of private information see generally P. 6, K. Lasky & A. Fletcher, *The Future of Privacy,* vol. 2 (London: Demos, 1998) at 93.

strengthen the foolproof identity verification process of the cardholder impeding misrepresentations.[158] Section 2.3.2 of the present chapter will thoroughly explain its promising significance to the air transport sector.

On the road towards worldwide acceptance and full implementation of smart cards, one issue often forgotten is that one of the most important factors for the programme to succeed is a cohesive harmonisation of standards among the participants in order to obtain a common interoperability of its applications. Hitherto, each player involved has been particularly keen on developing its own guidelines for a specific parochial use of smart cards, thereby missing the opportunity to exploit their full potential. However, there have been some efforts to lay down foundations for a harmonised smart card environment, predominately in Europe.[159] Thus, this thesis will proceed to analyse the European Smart Card Initiatives, focusing on the Dutch and Finnish programmes, and their joint effort within the European Smart Card Charter. Later their possible implication to the air transport sector will be examined.

2.3.1. European Smart Card Initiatives

In the early 1990's, smart cards with numerous different uses but without any interactivity started pouring into various countries in Europe, leading to a fragmented exploitation of their potential advantages. Businesses tried to implement a smart card system that properly would respond to their particular parochial usage and needs. The gathering of efforts in order to harmonise different initiatives became mandatory.

2.3.1.1. The Dutch Initiative

The Netherlands was the first country in Europe to understand the need for a joint effort approach to the problem. Thus, as a result of a conglomeration of efforts gathering the national trade association, the national union of banks, health insurers, combined public

---

[158] See generally N.K. Ratha & R. Bolle, "Smart Card Based Authentication" in A. Jain, R. Bolle & S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (Boston: Kluwer Academic Publishers, 1999) at 369.

[159] See generally W. Rankl & W. Effing, *Smart Card Handbook*, 2nd ed. (Oregon: Book News, forthcoming in September 2000).

transport organisations, the local and central government, the national consumers association, the national standards institution, and 25 information technology vendors, the National Chipcard Platform (NCP) was established in the Netherlands in 1993. It is indeed remarkable that the Dutch accepted the challenge to harmonise public and private initiatives through the NCP. Responding to an environment of a large number of independent, inconsistent chipcard programmes, the NCP emerged attempting to create the necessary background for an open chipcard system to ensure the multi-functional use a single smart card that would eventually allow the consumer to link different services from different providers. In order to achieve such a paramount task, the NCP has established amongst the balkanisation of players immersed in the market numerous agreements, standards, and guidelines interconnecting thereto. Ultimately the NCP sustains the designing of an electronic national identity smart card that could be used as a European travel document.[160] The latter is being developed following the international standards and the recommendations suggested by ICAO. In addition, understanding the risk to the privacy rights of individuals inherent in technological advancements, the Netherlands has enacted the *Wetbescherming persoonsgegevens*[161] or the Personal Information Protection Act.

2.3.1.2. The Finnish Initiative

Similarly, Finland is leading the way in the field of electronic identification for administrative purposes. In December 1999, the Finnish Population Register Centre introduced the Finnish electronic identification smart card (FINEID), which conceives the idea of joint applications for the public and private sectors, interconnecting numerous uses and services upon the customer's request.[162] The FINEID also has employer applications: granting access to the company's premises and its data network; municipal applications: permitting entrance to sports facilities, libraries, and public transportation; banking features: allowing access to personal accounts; and citizen applications: enabling the user to check and

[160] The Dutch electronic identification card also envisages the inclusion of biometric measurements, to be embedded in the smart card. See NCP, "Open Infrastructure for Chipcard Application" online: Http://www.ncp.nu/oic/brochureuk.html (date accessed: 30 June 2000).
[161] See *Wetbescherming persoonsgegevens*, 1999.
[162] Population Register Centre, News Release "Finnish Citizen Card and Electronic Identification" (22 November 1999), online: Http://www.vaestorekisterikeskus.fi/tied9931e.html (date accessed: 3 July 2000).

update his/her official records. Like its Dutch counterpart, the FINEID will act as a national electronic identification card that could be used as a travel document.[163]

Furthermore, Finland has gone a step further by enacting the Act on Electronic Service in the Administration[164] and the Identity Card Act,[165] aimed at instituting the desired legal framework for the interactivity of services and the FINEID. The former proposes to increase the promptness of administrative services, clearly establishing the rights, duties, and responsibilities of the administrative authorities and their customers in the context of electronic service.[166] The latter sets the legal grounds for the issuance of electronic identity cards. Thus, at the request of the cardholder, technical applications or data for various uses may be stored in the electronic identity card, meaning that each additional service is linked to the card only after the customer consents thereto.[167] Finally, the Finnish Population Register Centre will serve as the certificate authority, the trusted third party, for the electronic exchange of information among the participants by defining and issuing certificates.[168] The certificate authority could be held liable in damages for any loss arising from data having been erroneously entered into a certificate, but only when that authority has acted negligently.[169] However, the burden of proof is on the certificate authority.[170] Furthermore, Finland has enacted the *Personal Data Act of 1999*,[171] seeking to establish the necessary legal framework for the adequate protection of the individual's right of privacy. Remarkably, the Finnish initiative exemplifies a programme created within a legal framework where each party precisely understands its rights, duties, and obligations. Hence, a high degree of

---

[163] Population Register Centre, "Population information System in Finland" online: http://www.vaestorekisterikeskus.fi./hsteng.html (date accessed: 3 July 2000).

[164] See *Act on Electronic Service in the Administration*, 1999 online: http://www.edita.fi/sk/99/vihko159.pdf (date accessed: 22 August 2000).

[165] See *The Identity Card Act*, 1999, online: http://www.edita.fi/sk (date accessed: 22 August 2000)

[166] See *Act on Electronic Service in the Administration*, *supra* note 164, c. 1(1).

[167] See *The Identity Card Act*, *supra* note 167, s. 3.

[168] See *The Population Information Act*, Law 503, 1993 as amended by Law 527 in 1997, online: http://www.edita.fi/sk (date accessed: 22 August 2000). See also *The Population Information Decree*, 886 of 1993.

[169] See *Act on Electronic Service in the Administration*, *supra* note 164, c. 1, s. 15(1).

[170] The Act even addresses the issue of lost or stolen cards, stating that the card holder is not liable if he/she notifies the certificate authority that he/she has lost it or has reason to believe that the certificate is otherwise susceptible to unauthorised use. See *ibid.*, c.1, s.35 & 36.

[171] See *Personal Data Act*, Law 523, 1999, online: http://www.edita.fi/sk/vuosi99/index.html (date accessed: 22 August 2000). The latter is in accordance with the EC Directive 95/46 on Privacy Data Protection. See *EC Directive*, *infra* note 393.

confidence is given to customers, who in turn strongly favour the idea of one single smart card.

2.3.1.3. Applications to Air Transport

Both the Finnish and Dutch initiatives have achieved a milestone by laying out the compulsory standards and guidelines, and gathering players from a myriad of different sectors, public as well as private, for a truly multi-functional application of smart cards. Additionally, the Dutch and Finnish endeavours are vital elements of the European Smart Card Charter, which comprises a large number of public and private entities hoping to achieve harmonised use of smart cards within a broader European context. Thus, one of its primary goals is the creation of the Electronic European Identity Card, which could eventually replace the use of a passport on a regional basis, tremendously facilitating the traffic flow of passengers. The scenario is simplified by the fact that the majority of the countries involved, particularly Finland and the Netherlands herein examined, present similar levels of technical and legal harmonisation, whereby the necessary foundations have already been established. Hence, one can easily foresee the implementation of such endeavours on regional basis. The foregoing arguments support the belief of this thesis that, hitherto, Europe undoubtedly offers the best scenario for implementing electronic identification smart cards, replacing the use of passports, but solely on regional basis.[172] The preceding constitutes the landmark significance of the European smart card endeavours with direct implications in the air transport sector. In addition, the programmes of Finland and the Netherlands have included biometric measurement, thereby enhancing the capabilities of smart cards.

2.3.1.4. Critical Appraisal

In spite of major achievements and improvements with smart cards directly improving the facilitation scenario in air transport by means of automation, this author

[172] *A contrario*, the scenario in the United States is completely dissimilar with respect to the establishment of an identification card that could ultimately be used as a travel document on a national basis. Americans fear that by giving up personal information in order to establish a national identification programme, it will represent an undesirable government intrusion into the individual's personal life. For a comprehensive

believes that such accomplishment is somewhat fractional. Some significant players, such as the United States, have a considerably lower level of standardisation, both from a technical and legal perspective. The possible expansion of electronic identification smart card decreases with the participation in air transport of less developed countries. Therefore, complete passport replacement remains utopia.

2.3.2. Biometric Applications in Smart Cards

As a process of human recognition, biometrics represent an automated measuring method through which an individual's unique physical characteristic or personal trait is compared to that characteristic or trait previously stored in the database for personal recognition of that individual.[173] Similarly, the International Biometric Association (IBA) defines "biometrics" as "a measurable physical characteristic or person-related behaviour that can be used to automatically ascertain a person's identity, or to verify the submitted identity of a person".[174] Furthermore, biometrics unique characteristics are two-fold:

- Behavioural characteristics, including dynamic habits such as voice pattern and signature. Although stable in nature, their features are subject to change.
- Physical characteristics, encompassing facial features, retinal vein pattern, iris pattern, heat pattern in the face, ear shape, hand geometry, personal body odour, vein measurement, finger imaging.[175] These features are theoretically not subject to change.[176]

2.3.2.1. Biometric Scanning

---

study on US national ID cards and privacy issues, see especially J.W. Eaton, *Card-Carrying American* (Totowa, New Jersey: Rowman & Littfefield Publishers, 1986) at 11.

[173] See J.D. Woodward, "Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometric Blueprint" (1997) 59 U. Pitt. L. Rev. 97 at 99, citing B. Miller, *Everything You Need to Know About Automated Biometric Identification.* See also *Hearing on Biometrics and the Future of Money Before the Subcommittee On Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105 Cong., 2nd Sess. (1998) (particularly the statement of Jeffrey S. Dunn, Chairman, Biometric Consortium).

[174] See J. Van Arkel & A. van der Tuin, "Who Did You Say You Were" in F. Knopjes & P.J. Lakerman, eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999) 117 at 124.

[175] See generally L.C. Jain, U. Halici & I. Hayashi, eds., *Intelligent Biometric Techniques in Fingerprint and Face Recognition* (Portland: Press International Series on Computational Intelligence, 1999).

Biometric scanning is the method of automatically asserting to an individual's identity through a computer system containing previously collected biometric measurements.[177] The first step of the process comprises the collection of a unique biometric characteristic of an individual, obtained with his or her own consent. During the collection process, the data capture device must remain free from any external interference, thereby ensuring a non-contaminated environment. In addition, to implement biometrics, a centralised storage system must be used, as opposed to a decentralised one, which in the latter case might include adding to the number of players involved, as well as increasing the legal relations therefrom.

Once the information is collected, it is stored in the computer system, which generates a digitised code for the unique biometric characteristic; this code can also be transmitted to a smart card. In this case, the individual approaches a reading device where the system prompts him to insert his smart card and provide the biometric characteristic as well; hence, the identity of the individual is verified against the database, answering the question "Are you who you claim to be?"[178] This process could be an invaluable tool for speedily authenticating the identity of persons in numerous fields.[179] As a matter of fact, the US Government has started implementing biometric measurements in the welfare system as a means of counterattacking the tremendous amount of fraud brought by recipients, which results in significant economic losses for the US Government.[180]

Similarly, the Dutch Government has undertaken pilot biometric programmes to test the feasibility of having cards for drug addicts, asylum seekers, Parkinson patients, and patrons of the Schiphol National Airport. Other foremost fields of applications of biometric technology as a means of rapid identity verification include, *inter alia*, driver licenses, authentication of inmates in prisons, and national identity card programmes.[181] The latter has been envisioned by a large number of countries, primarily in Europe, as an adequate, cutting-

---

[176] See E. Bovelander & R. van Renesse, "An Introduction to Biometrics" in F. Knopjes & P.J. Lakerman, eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999) 13 at 19.
[177] See Woodward, *supra* note 173 at 100.
[178] *Ibid.*
[179] See also Biometric Consortium, "Government Applications and Operations" online: http://www.biometrics.org/REPORTS/CTSTG96 (date accessed: 19 August 2000).
[180] See J.J. Killerlane, III, "Finger Imaging: A 21st Century Solution to Welfare Fraud at our Fingertips" (1995) Fordham Urb. L.J. 1327.
[181] See R. Heitmeyer, "Biometric ID and Airport Facilitation" *Airport World* 5:1 (March 2000) 18.

edge instrument to empower their citizens with valid identification cards that could be used as travel documents on a regional basis.

2.3.2.2. Applications to Air Transport

In the air transport sector, passengers could use biometric scanning at immigration passport control lines and customs queues, speeding up the pace of air traffic flows considerably.[182] Accordingly, Annex 9 recommends Contracting States using internationally standardised formats for biometric and digitised photographic data, which could hasten the identification of the document holder.[183]

2.3.2.3. Critical Assessment

Despite the advantages, the development of biometric measurement devices embedded in smart cards, raises numerous concerns worth analysing. Firstly, a large number of commentators have noted that biometrics produce a negative public reaction when the individual is asked to be scanned for the purpose therein pursued; hence, there is a psychological acceptance factor, the so-called social stigma, that institutions undertaking such projects cannot ignore.[184] Consequently, one of the key issues when implementing biometric initiatives is to develop a user-friendly system to avoid their social rejection by users.[185] Particular attention should be given to selecting the type of biometric measurement device to be applied, which should be based on its intended used. Secondly, as noted by some commentators, biometrics may compromise the physical and information privacy of the individual, an issue that will be thoroughly discussed in Chapter 4.[186]

---

[182] In this respect, a detailed explanation of the INSPASS programme carried out by the US Immigration and Naturalisation Service will be addressed in Section 2.4.2 of the present chapter.

[183] See *Annex 9*, *supra* note 35, recommended practice 3.5.10. Similarly, ICAO has undertaken several studies examining the feasibility of including biometrics into its machine-readable travel documents. See ICAO, *Amendment to informative annex on machine assisted document security verification*, WP/8 presented at TAG-RT/11; 1-3 September 1999; ICAO, *Enhancement of specifications of displayed feature(s) on MRTDs*, WP/10, presented at TAG-MRTD/11, 1-3 September 1999; ICAO, *Request for information – Biometric recording and verification technologies, machine verification technologies and document security devices*, WP/9 presented at TAG-MRTD/10, 18-20 February 1998.

[184] See Killerlane, *supra* note 180 at 84; Woodword, *supra* note 173 at 102.

[185] See L.J. McGuire, "Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy" (2000) 33 Akron L. Rev. 441 at 446-448 (expressing the social concern of the implementation of biometric identifiers in the banking industry).

[186] See *ibid.*, at 480.

2.4. Smart Cards Applications to Air Transport

This section will examine how smart cards are being implemented in air transport, particularly concentrating on the efforts undertaken by air carriers and the endeavours carried out by government attempting to include biometric measurement devices in smart cards, aiming to streamline immigration and customs formalities. With respect to the latter, the US and Canadian experience will be exposed. Finally, this section will address the Simplifying Passenger Travel programme as the desirable, ultimate goal to achieve automation in facilitation of air transport.

2.4.1. Air Carriers' Endeavours

In 1996 American Express and American Airlines conducted a trial programme with a group of 5,000 frequent flyers, providing them with an American Express corporate credit card containing an IBM chip. This card enabled the passengers to check themselves through special kiosk gate readers at domestic airports when travelling using an electronic ticketing.[187]

---

[187] See J. Levere, "The Smart Airlines Take Credit Cards" *Airline Business* (March 1998) 79. See generally IBM, "American Express Licenses Smart Card Multiple Application Framework to Leading Industry Players" online: http://houns54.clearlake.ibm.com/solutions/travel/trapub.nsf/detailcontacts/American_Express_licenses_smart_card_multiple_application_framework_to_leading_industry_players?opendocument&detail=1 (date accessed: 23 June 2000); P. Harrop, "Playing the Smartcard" *Air Transport World* 14:10 (October 1998) 81; J. Gallacher, "Playing Your Cards Right" *Airline Business* 15:8 (August 1999) 46. For business articles with respect to electronic ticketing see generally Airline Industry Information, "AII Provides a Roundup of News not Reported Elsewhere" (September 1997); Airline Industry Information, "Ticket Sold Online to be Less Flexible than Those Paid for Through Travel Agents/Direct Under New Rules" (November 1999); Airline Industry Information, "US Travel Agents Complain of Internet Sales" (October, 1997); Airline Industry Information, "Travel Agents Being Hit by Growing E-ticketing Popularity" (July 1999); Airline Industry Information, "US Airways Expands Electronic Ticketing to Canada" (October 1997); Airline Industry Information, "IBM work with IATA to Improve Electronic Ticketing" (August, 1999); Airline Industry Information, "Asian Economic Problems are Hampering E-commerce Uptake in Aviation Industry" (May 1999); Airline Industry Information, "Electronic Sales Overtake Paper Sale at United Airlines" (June 1999); Airline Industry Information, "NW Introduces E-ticketing for US/Canada to Asia Routes" (July 1999); Airline Industry Information, "Electronic Ticketing Becoming More and More Popular" (July 1999); Airline Industry Information, "America West, Continental Introduce Interline E-ticketing" (October 1999); Airline Industry Information, "JAL to Offer E-ticketing Service" (April 2000); Airline Industry Information, "Chinese-Taiwanese Ticketing Agreement Arranged" (July 1997); Airline Industry Information, "Airlines Eager to Promote Online Ticket Sales" (October 1998); Airline Industry Information, "Unisys Introduces New Ticketing Product" (July 1997); Airline Industry Information, "Airlines on the Internet" (January 1997); Airlines International, "IBM Providing Travel Solutions in a Fast Changing World" (January 1997); Airlines International, "The Crazy Huge Thing Called the Internet" (January 1997); Airlines International, "Getting a Grip on the Internet" (January 1997); Airports,

Other airlines, *inter alia*, Continental, Delta, Lufthansa, and Air France, have undertaken endeavours to develop the use of smart cards in air transport.[188] Although originally conceived to be used in conjunction with electronic ticketing, smart cards also provide the means for air carriers to link other services to the passenger such as paid phones, internet access, entrance to VIP lounges, and sale of in-flight duty-free items. Hence, the industry players have also introduced co-branded cards.[189] Similarly, the European Union has conceived the idea of implementing smart cards tailored to a multi-ticketing system, which will make it technically possible to book a journey on a variety of transport systems across Europe, pay for it and, using the same card, print a personalised through-ticket showing a complete itinerary.[190] However, air carriers' smart card programmes at present do not reach the large majority of passengers. They are targeted at a selective, experienced, elite group of the most frequent travellers among the airlines' clientele.

Understanding the need for certain guidelines, IATA, through its Resolution 791, has dictated specifications for Airline Industry Integrated Circuit Cards (ICCs), addressing the minimum standards necessary for the issuance of a smart card to facilitate the expansion of

---

"Continental Begins Self-Ticketing Service at Airports" (April 1995); Airports, "United Now Offering Electronic Ticketing Nationwide" (September 1995); Airports, "United to Offer Electronic Ticketing on International Flights" (November 1995); Aviation Week & Space Technology, "Online Ticket Sales Soaring at Southwest"(March 2000); C. Baker "British Airways Moves Towards Internet Network" *Airline Business* (February 2000); BCBR.com, "Tips for Travel with Electronic Airline Ticketing" online: http://www.bcbr.com/aug96/eside2.html (date accessed: 17 May 2000); D. Blank, "Raising the Internet Stakes" *Airline Business* (September 1999); A. Borgo & T. Bull-Larsen "Losses: What Losses?" *Airline Business* (August 1998) 54; Canada Newswire, "Air Canada Introduces Electronic Ticketing to Bermuda" (February 1999); Canada Newswire, "Air Canada Expands Electronic Ticketing Throughout North America" (November 1998); C. De Pommes, "Are you IT-Compatible?" *Airline Business* (July 1998) 26; J.M. Feldman, "Cyberspace Direct" *Air Transport World* (August 1996); J.M. Feldman, "E-commerce: The Future is Now" *Air Transport World* (November 1999; F.Phillip, "Wheeling out the Service" *Airline Business* (January 1997) 40; P. Flint, "Bigger than the Internet?" *Air Transport World* (September 1998) 54; P. Flint, "Cyber Hope or Cyber hype?" *Air Transport World* (October 1996) 25.

[188] See IATA, "Airline Industry Smart Card Developments" online: http://www.iata.org/smartcard/smartcard.html (date accessed: 23 June 2000).

[189] However, some air carriers' officials remain sceptical about full-scale implementation of smart cards in the airline industry, especially the idea of one single empowered card, primarily because it could certainly work against one of the main objectives of electronic ticketing in the airline industry, namely, eliminating the intricate re-issuance process that must take place when an air traveller loses his original ticket booklets. The argument goes that if the air passenger loses the smart card, the cycle starts again. Notwithstanding the foregoing discussion, this thesis strongly supports the idea that the full implementation of smart cards has a significant role to play in the air transport industry, where the previous argument constitutes only one single possible drawback.

[190] See "Intermodality: Forward Towards an Integrated European System" *Transport Europe* 58 (19 January 1996).

electronic ticketing.[191] Accordingly, IATA has also strongly supported the implementation of the "Simplifying Passenger Travel" programme, which will be further analysed later. [192]

2.4.2. US INSPASS

In 1993, 483 million people entered the United States by land, sea or air — almost twice its population. To cope with the exceptionally large number of passengers arriving in the United States, the US Immigration and Naturalisation Service has been experimenting with automation procedures for purposes of inspection.[193] Within this context, the US Immigration and Naturalisation Service introduced the INS Passenger Accelerated Service System (INSPASS) as a pilot programme at JFK Airport in May 1993. By granting other means of expedited self-inspection without human intervention, the main objective of the pilot programme has been to remove frequent business travellers, considered to be low-risk passengers, from inspection lines, thereby accelerating the flow of traffic. Additionally, the programme combines an INSPASS card the size of a credit card, with a hand geometry biometric image containing the passenger's physical characteristics.[194] This biometric measurement includes a three-dimensional record of the hand or fingers, which is then converted into a less than 10-byte digitised code.[195]

The passenger is required to pass through an INSPASS kiosk similar to an ATM. After inserting his card into the kiosk, the system prompts the passenger to align his hand in the hand geometry reader for identity verification. Then the system proceeds to match the identity of the passenger through biometric authentication. If the identity is validated, the

---

[191] See IATA, *supra* note 188; CNN, "Smart Cards: The Hassle-free Future of Travel?" online: http://cnn.com/tech/computing/9903/26/t_t/e.travel (date accessed: 23 June 2000); K. Magnay, "Creative Passenger Processing Options on Show" *Aviation Informatics* (November 1996) 21; J. Stillwell, "Will Smart Cards Take Flight?" *Aviation Informatics* (November 1996) 27.

[192] For comprehensive guidelines on using smart cards for electronic ticketing, see generally P. Bradley, "Implementing Airline Electronic Ticketing Using Integrated Circuit Cards" (D. Applied Science Thesis, Dublin: Dublin Institute of Technology, 1999)[unpublished].

[193] See R. Hays, "INS Passenger Accelerated Service System (INSPASS)" *Biometric Consortium* online: http://www.biometrics.or/epots/inspass.html (date accessed: 26 June 2000).

[194] See Department of Justice Immigration and Naturalization Service, "INS Passenger Accelerated Service System" online: http://www.ins.usdoj.gov/graphics/publicaffairs/factsheets/passfs.html (date accessed: 26 June 2000). See also M. Dinning, "Transportation" in C. Allen & W.J. Barr, eds., *Smart Cards* (New York, McGraw-Hill, 1997) 177 at 191.

[195] See Woodword, *supra* note 173 at 105.

kiosk prints an I-94 form receipt for the passenger. Subsequently, the gate opens and the passenger continues on his journey. The entire process takes between 15 to 20 seconds.[196]

The INSPASS programme is only open to citizens of the United States, Canada, Bermuda, and Visa Waiver Pilot Programme (VWPP)[197] countries travelling to the United States on business for visits of no longer than 90 days, three or more times a year, who do not possess criminal records. The programme is only offered at certain US airports.

2.4.3. CANPASS

Similarly and as a consequence of the Canada-United States Accord on Shared Borders, CANPASS has been launched in an effort to facilitate and promote tourism and trade, but solely between those two countries.[198] Although bearing the same objective as its US INSPASS equivalent, which is to streamline customs and immigration clearance for low-risk passengers, CANPASS only targets citizens or permanent residents of Canada and citizens or resident aliens of the United States. Hence, its scope of operability and application is considerably smaller, as opposed to the INSPASS initiative, which through its visa waiver pilot programme includes a large number of countries. The card has an annual membership fee of $ 50.[199] The CANPASS programme uses an optical smart card encoded with the individual's hand geometry and fingerprint, which can be tested at kiosks located at some international airports;[200] *contrario sensu*, the INSPASS system uses solely hand geometry. The foregoing could contribute to the development of rather different systems, with no interoperability between them. Should each country adopt its own standards and select a different biometric characteristic feature for its intended application, it would be tantamount to the formation of an isolated parochial initiative without the possibility of global implementation. Therefore, the need to develop standards for automated inspection

---

[196] See *ibid.*, at 106.

[197] Currently Andorra, Argentina, Australia, Austria, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, San Marino, Norway, Spain, Slovenia, Sweden, Switzerland, and the United Kingdom are members of the VWPP.

[198] See Canada Customs and Revenue Agency, "CANPASS – Airport Extending Border Services" online: http://www.ccra-adrc.gc.ca/E/pub/cp/rc4062ed/rc4062ed.html (date accessed: 15 August 2000).

[199] See Canada Customs Revenue Agency, " Guidelines and General Information" online: http://www.ccra-adrc.gc.ca/E/pub/cm/d259/d259ed.html (date accessed: 15 August 2000).

[200] See J. Stillwell, *supra* note 191 at 26.

worldwide was crystallised with the congregation of numerous organisations and institutions at the Future Automated Screening for Travellers (FAST). However, its achievements are yet to be seen.

2.4.4. Simplifying Passenger Travel

On 28 May 1998, the Airport Council International (ACI), the World Custom Organisation (WCO), the Control Authorities Working Group (CAWG), the Air Transport Users Council (AUC), ICAO[201] and IATA held their first meeting on "Simplifying Passenger Travel" (SPT), aimed at eliminating unnecessary forms for landings and departures, eradicating exit controls by customs and immigration authorities, abolishing tax collection procedures, promoting API systems, and last but not least, convincing control authorities to fully accept electronic ticketing.[202]

The SPT Vision programme desires to implement a "one-stop check" concept with multifunctional, interactive use of a machine-readable biometrics smart card, from the moment of making a reservation enquiry, to obtaining an electronic ticket[203] at departure

---

[201] Although ICAO is also member of the SPT initiative, the leading role is performed by IATA, reflecting the private entrepreneurial approach of the programme.

[202] For articles addressing legal issues that implementing electronic ticketing rises see generally R.I.R. Abeyratne, "The e-ticket and trademark issues of computerized airline ticketing" (2000) 5:2 Tolley's Communications L. 58; R.I.R. Abeyratne, "Auctions on the Internet of airline tickets" (1999) 4:1 Tolley's Communications Law 22; C.E. Dubuc "Air Travel, Tourism, Electronic Tickets and the Warsaw Convention in Cyberspace" (1997) 22:6 Air & Sp. L. 291; D.M. Fiorita, "The Warsaw Convention and Electronic Ticketing: Neither Ticketless nor Paperless" (1997) XXII Ann. Air & Sp. L.159; P. Lyck & B.A. Dormic, "Electronic Ticketing under the Warsaw Convention: The Risk of 'Going Ticketless' on International Flights" (1997) 22:1 Air & Sp. L. 13; R.D. Margo, "Legal Aspects of Electronic Ticketing" (1997) XXII Ann. Air & Sp. L. 177; P. Martin, "Phone in, Turn up, Take-off, A Look at the Legal Implications of Self-service Ticketing" (1995) 20:1 Air & Sp. L. 189; P. Martin, "Ticketless (but not documentless) travel" (1995) 14:6 Lloyd's Aviation L. 1.

[203] For interesting industry articles concerning electronic ticketing see generally J. Gallacher, "Phone Alone" *Airline Business* (May 1999) 43; J. Gallacher, "Easy Does it" *Airline Business* (December 1997) 61; J. Gallacher, "Holding the Pieces Together" *Airline Business* (January 1998) 28; T. Gill, "Sabre" *Airline Business* (January 2000); M. Gormley, "Aviation on the Internet" *Business & Commercial Aviation* (September 1995) 76; C. Jirasakunthai, "Qantas-BA to Launch E-ticketing" *Nation* (May 1999); L. Jones, "Skating on Thin Ice" *Airline Business* (February 1997) 36; J. Judge "No Free Ride for Automatic Ticketing" *Aviation Informatics* (April 1994); J. Levere, "On-Line, A new Web Challenger" *Airline Business* (November 1998) 49; J. Levere, "Agents of Change" *Airline Business* (August 1997) 52; J. Levere, "Netting a Bargain" *Airline Business* (August 1999) 18; J. Levere, "No Ticket to Ride Catching on Fast" *Airline Business* (September 1997) 122; J. Levere, "Low Fares Capture More Web Sales" *Airline Business* (January 1998) 62; J. Levere, "Internet Pursuit Heats Up" *Airline Business* (December 1998); J.

gate, to passing through immigration and customs formalities upon arrival, to baggage pick-up — a total "hassle-free travel journey".[204]

In an ideal scenario, by using a smart card a passenger could make his own reservation through his personal computer at home by inserting such data as seat preference, nationality, dietary concerns, disabilities, frequent-flyer programme number, desirability of long distance phone cards, hotel bookings, access to bank accounts, and car rental request. The system would then display the passenger's itinerary, any destination document requirements, conditions of the contract performed, and ticket notices; it would also be capable of downloading all travel expense information, enormously simplifying the passenger's expense reporting.[205] Then, the system would generate an electronic ticket to be paid for using the passenger's smart card; the same would be possible for excess baggage, parking fees, and airport related taxes. Once at the airport the passenger would proceed to a one-stop gate, a so-called "kiosk", where by inserting his smart card and entering the flight number the passenger could complete a biometric scan. If the biometric verification were approved, the passenger would receive an itinerary receipt and proceed to board his flight. In

---

Levere, "Alaska Offers Internet Check-in" *Airline Business* (April 2000); J. Levere, "Paperless Journey – Electronic Ticketing" *Airline Business* (January 1995); M2 Press Wire, "Electronic Ticketing Now Available on Air Canada's Caribbean Routes" (July 1999); M2 Press Wire, "Cathay Pacific Launches Electronic Ticketing" (January 1998); M2 Press Wire, "Delta Air Lines Introduces Electronic Ticketing to and from Latin America" (April 1999); M2 Press Wire, "United Airlines and Air Canada Introduce Airline Industry's First Inter-Airline Electronic Ticketing" (June 2000); M2 Press Wire, "American & United Airlines to Develop Interline Electronic Ticketing Product" (May 1998); K. Osborn, "Spinning a Web" *Airline Business* (January 2000); K. O'Toole, "Gaining an Edge" *Airline Business* (November 1998) 70; K. O'Toole, "Getting the E-price Right" *Airline Business* (December 1999); K. O'Toole, "Up to the Minute" *Airline Business* (December 1999); K. O'Toole, "IT Trends Survey" *Airline Business* (August 1999); J. Ott, James, "Airlines Using Web for More than E-ticketing" (March 2000); PR Newswire, "United Airlines' E-Ticket (SM) Service Lands in Chile and Venezuela" (June 1999); PR Newswire, "Delta air Lines Introduces Electronic Ticketing with Delta Connection Carriers" (April 1999); Pr Newswire, "Corporate Travel Decision-makers Endorse Electronic Ticketing for Air Travel" (February 1996); E. Russel-Wailling, "The Ticketless Transition" *Airport World* (July 1997); N. Schwartz, Nancy & M. Zea, "Surfing the Value" *Airline Business* (July 1999) 68; A. Velocci, Anthony, "Southwest to Tap Internet for Ticketless Travellers" *Aviation Week & Space Technology* (June 1995); K. Walker, "The King of Low-cost" *Airline Business* (June 1999) 38; K. Walker, "Proceed with Care" *Airline Business* (June 1997) 70; B. Walters, "Airport Go-faster Strips" *Jane's Airport Review* (October 1994); R. Whitaker, "Airline Revolution Gathers Pace" *Airline Business* (August 1998) 7; R. Whitaker, "Channel your Sales Energies" *Airline Business* (April 1998); IATA, "IINET – IATA Service for the Air Transport industry" online: Http://www.iata.org/iinet/index.html (date accessed: 17 May 2000); IATA, "Electronic Ticketing, Airline Industry ET Developments" online: Http://www.iata.org/eticket/eticket.html (date accessed: 17 May 2000).

[204] See IATA, "Simplifying Passenger'Travel" online: http://www.iata.org/smartcard/article1.html (date accessed: 24 June 2000). See also Jeanniot, *supra* note 12 at 10; K. Magnay, "Creative Passenger Processing Options on Show" *Aviation Informatics* (November 1996) 21.

[205] See J. Levere, "The Smart Airlines Take Credit Cards" *Airline Business* (March 1998) 79; S. Fenner, "Playing Smart Card" *Airline Business* (October 1998) 83.

case of baggage, the passenger would place them on an automated device that would record the weight and number, and engender a traceable baggage tag containing a radio frequency chip. Upon arrival, the passenger would undergo another biometric check using the smart card before collecting his baggage. Throughout the entire passenger's journey all parties involved would be linked electronically, a capability that would allow the passenger's data to be shared among the participants on a "need to know" basis.[206] Since the SPT initiative involves such a large amount of data and a variety of players, the degree of security reliance of each of the programme's components is vital to avoid any possible "informational leaks". Notwithstanding the "need to know" principle, the SPT participants would be handling, *inter alia*, the passenger travel details, credit records, and personal data. Mishandling or misusing the aforesaid data could create awful scenarios.[207] One, one can imagine, for instance, one of the participants of the STP leaking the client's credit card details and other personal data, and that such information being captured by lawbreakers. These individuals would be in a perfect position to assume the data subject's identity for financial gain. This particular emerging fraud is called "Identity Theft" in the United States, and numerous cases have been recently reported whereby these criminals have caused exorbitant financial losses.[208] Hence, the technological infrastructure of the SPT initiative must be constructed in such a way as to avoid informational leaks and to ensure the maximum level of data security in order to grant the data subject the necessary guarantee of a "personal information sanctuary".[209] This thesis supports the idea that one of the most significant factors when structuring the SPT initiative will be the proper implementation of a trustee party or institution to be in charge of administrating and co-ordinating the sharing and use of personal data on a need to know basis. Should there not be any trustee, the system runs unaffordable risks.

---

[206] See M. Hawes, "For Growth You Need Vision" *Airlines International* 5:1 (January 1999) 28 at 29.
[207] Commentators have identified that the mishandling of personal data comprises a dual independent facet: 1) the negligent processing of data, and 2) the unlawful processing of data. See Kraus, *infra* note 432 at 85.
[208] See K. Provenza S., "Identity Theft: Prevention and Liability" (1999) 3 N.C. Banking Inst. 319 at 323. The US government has become so concerned with the implications of these frauds that it has introduced the Identity Theft Prevention Act of 2000, which is currently under examination at the US Congress, in an effort to prevent fraud in consumer credit transactions and credit in general. See *Identity Theft Prevention Act of 2000*, Bill 2328, 106th Congress.
[209] See generally J. Konicek & K. Little, *Security, ID Systems and Locks*, (Boston: Butterworth-Heinemann, 1997) at 27.

While the application of advanced technology as envisioned in the SPT initiative brings marvellous benefits to its users, it also increases the risk of personal monitoring and surveillance.[210] This privacy concern issue, will be examined hereafter.

Although raising a myriad of different legal questions whose assessment will be carefully examined hereafter, the SPT entrepreneurial-driven initiative clearly represents the ideal automation implementation concept in air transport. Its objective is to ultimately ease the whole passenger journey, not just some elements, abolishing bureaucratic formalities, unnecessary inconveniences, and significantly contributing to facilitate air traffic flows.[211] By bringing together at the negotiating table diverse players involved in the passenger's journey, *inter alia*, government authorities, airport administrators, consumers, and airline operators, the SPT initiative could have a substantial impact on air transport were it to be fully implemented. But the question then arises as to what extent the SPT initiative would achieve worldwide application and acceptance. This thesis defends the idea that this private endeavour could be implemented to a considerable degree in the near future, but only on a regional basis or for very specific air transport markets. The *rationale* behind this statement is that the full implementation of such initiatives are tremendously burdensome due to their cost, which a large number of countries are not in a position to afford. The response of the less-developed countries to such initiatives is yet to be tested.

Despite the cumbersome task of assembling a large number of different players in the SPT initiative under a common objective, one commentator has mentioned that the official legal mechanism to achieve such goals would seem to be through the structure established by Annex 9 of the Chicago Convention. Then ICAO would be called to play the leading role. Albeit an ideal goal, in reality ICAO constitutes a rather complex international body balancing the interest of its 185 members, wherein most decisions are reached through prolonged consensus deliberations, thereby encumbering the quickness of their applications. The pragmatic attitude pursued by the private entrepreneurial sector would best suit the

---

[210] See generally D. Johnston, D. Johnston & S. Handa, *Understanding the Information Highway* (Toronto: Stoddart Publishing, 1995) at 193; D. Lyon & E. Zureik, "Surveillance, Privacy, and the New Technology" in D. Lyon & E. Zureik, eds., *Computers, Surveillance, and Privacy,* (Minneapolis: University of Minnesota Press, 1996) at 1.

[211] See "Insight on IATA" *Airlines International* 4:5 (September 1998) 54.

necessities of the SPT initiatives, although public supervision at arm's length by international organisations or national governments would be highly advisable.

2.5. Global Assessment of Automation Initiatives

Endeavours to implement automation in facilitation of air transport characterise a superlative effort currently undertaken by numerous industry players. This thesis acknowledges such a significant accomplishment, which is indeed crucial for the interest of continuing the development of the industry to confront emerging trends of air traffic growth. However, it has been said previously that most of these initiatives, particularly the ones carried out by the private sector, only target specific markets for a rather elite type of passenger, hence, lacking massive global application. Indisputably, ICAO's MRTDs programme has achieved a larger degree of worldwide compliance therewith. However, unless financial assistance is provided to a large number of developing countries, full implementation of MRTD will not be accomplished in the near future.

On the other hand, one can certainly question to what extent the entrepreneurial sector is keen on developing automation devices that could be implemented in a larger number of markets, rather than concentrating solely on the most profitable ones. Undoubtedly, developing countries will rarely be included in these initiatives because of the enormous financial difficulties they are experiencing at present.

This thesis sustains the idea that the endeavours herein described could be considerably implemented in developed markets on a regional basis, especially European electronic identity cards, which are not oriented to a selective group of users. Its application could then reach a larger number of persons involved. Consequently, its result could considerably have an impact on these automation initiatives. The SPT and CANPASS programmes will most likely continue to be elitist, primarily because the United States and Canada face tremendous immigration problems that could thwart the success of these endeavours should they be implemented on a larger scale. Another major threat to these initiatives is the risk of creating a fragmented automation environment similar to the frequent flyer mileage cards, where there is a total lack of interactivity, creating for the passenger the inconvenience of having to carry along numerous different cards from different service

providers. Unless harmonisation is achieved in this respect, these initiatives will miss the opportunity of reaching their intended objectives, thereby not achieving global application.

The foregoing supports the argument that by implementing these automation initiatives, facilitation in air transport will be achieved to a substantial degree, but the presence of formalistic and bureaucratic procedures at immigration and customs controls will still remain on a global basis, because a large number of countries continue to view those requirements as part of their sovereignty and *potestas*.

Chapter Three

Banking, Financial, and Evidentiary Issues

This Chapter will analyse certain legal issues that have arisen due to the SPT programme and the development of the electronic identity travel cards. The first section will briefly deal with banking and consumer laws in the United States, since this automation programme conceives the smart card empowerment with credit card capabilities. Special attention will be drawn to possible unauthorised uses thereof. The second section will address the issue of inadmissible passengers generated by implementing smart cards in air transport; the legal framework of the provisions of Annex 9 will be mentioned in this regard. The primordial purpose pursued herein is to identify the legal issues, to establish their links with these initiatives, and to pinpoint some relevant aspects of particular significance for their full application, hence contributing to the formation of a greater awareness of these problematic matters.

3.1. Banking, Financial, and Consumer Law Implications

Implementing automation initiatives to facilitate air transport involves the congregation of numerous players from diverse sectors, as explained previously. For instance, the SPT initiative envisions the development of smart cards with credit or debit card functions as one part of its vast programme, directly affecting banking, financial and consumer regulations. In this respect, the legislation of the United States has been selected to provide examples and legal conclusions from implementing the SPT.

At the outset of the discussion it is mandatory to mention that the credit card regulatory framework varies considerably in different part of the world. In the so-called "developed countries", there is a tendency to favour the adoption of consumer-oriented legislation, whereas the less-developed countries, are rather keen on relaxing their legal framework, hence favouring the entrepreneurial sector, which has considerably more bargaining power.[212] Undoubtedly the expansion of credit cards has radically shifted

[212] For interesting studies on credit cards see generally D.G. Reynoso, *Sistema de Tarjeta de Crédito* (Buenos Aires: Roberto Guido, 1997); C.G. Villegas, *Compendio jurídico, Técnico y práctico de la actividad bancaria* (Buenos Aires: Editorial Depalma, 1990); R.A. Mugillo, *Tarjeta de Crédito* (Buenos

consumer transactions of the ordinary individual. Today one in every five inhabitants of the world possesses a credit card; this statistical figure supports its dominant role.[213] Commentators have noted that the flourishing usage of credit cards is owed to their convenience and the fact that they have emerged in an environment with high levels of protection.[214] This thesis agrees with the first statement, but dissents with the last, primarily because on a global basis the levels of protection vary greatly. Some countries like Paraguay, for instance, offer very little consumer protection; nevertheless, credit cards have boomed there since their early inception in the market.[215] It is safe to assert that credit cards' handiness outweighs their considerable risk.[216]

3.1.1. Credit Cards *vis-à-vis* Debit Cards

Perhaps one of the most important matters for industry players to clarify when establishing the business infrastructure of the SPT is whether the smart card has credit or debit functions, and subsequently, whether the card has been issued by a banking institution or a non-banking institution. The foregoing will determine which specific legislation will govern its implications in the market and its relationship with consumers. The distinctive line between debit and credit cards is rather difficult to draw, primarily due to the constant interaction and combination of services linking institutions and customers. However, both systems involved a tripartite contractual arrangement connecting customers, financial institutions, and merchants.[217] A debit card, also regarded as a cash card or an asset card, links the bearer as a customer with the particular financial organisation where he possesses

---

Aires: Editorial Astrea, 1994); J.A. Moreno Rufinelli, *La Tarjeta de Crédito* (Asunción: Intercontinental Editora, 1994); T. Drury & C.W. Ferrier, *Credit Cards* (London: Butterworths, 1984); P.E. Sayer, *Credit Cards and the Law: An Introduction* (London: Fourmat Publishing, 1988); T.D. Steiner & D.B. Teixeira, *Technology in Banking* (Homewood, Illinois: Business One Irwin, 1990) at 112; Y. Valcin, *L'argent électronique: quitte ou double* (Lac Beauport, Quebec: Atelliers Graphiques Marc Veilleux Inc., 1985)

[213] See A. Piera, "La Tarjeta de Crédito" (1998) 8 Revista Juridica U. Católica de Asunción 269.

[214] See J. Kaufman Winn, "Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment Systems" (1999) 14 Berkeley Tech. L.J. 675 at 687.

[215] See Piera, *supra* note 213 at 270.

[216] See generally D.N. Chorafas, *Electronic Funds Transfer* (London: Butterworths, 1988) at 336; E.H. Solomon, ed., *Electronic Funds Transfers and Payments: The Public Policy Issues* (Boston: Nihoff Publishing, 1987) at 13; L. Mandell, *Credit Card Use in the United States* (Ann Arbor, Michigan: The University of Michigan Press, 1972) at 94; D.S. Evans & R. Schmalensee, *Playing with Plastic* (Cambridge, Massachusetts: The MIT Press, 1999) at 1; L. Mandell, *The Credit Card Industry* (Boston: Twayne Publishers, 1990).

[217] See I.J. Sloan, *The Law and Legislation of Credit Cards: Use and Misuse* (New York: Oceana Publications, 1987) at 5.

deposited funds.[218] When the cardholder carries out a transaction the amount is debited from his account, to be subsequently transferred to the merchant's account.[219] With in a credit card the issuer provides short-term credit to the cardholder, who then has to repay the charges incurred by his transactions plus interest, which can vary considerably among issuers and markets.[220]

3.1.2. Unauthorised Uses

Another major question when dealing with credit or debit cards constitutes the level of consumer protection given to the individual against unauthorised uses. In this respect it is key to differentiate three distinctive concepts. The "authorise use" of a credit or debit card refers to transactions performed or approved by the cardholder; "misuse" denotes the exceeding employment of the card by its bearer beyond its credit limits; and "unauthorised use" implies the unlawful utilisation of a card by person other than the cardholder.[221] The latter category is of paramount importance for the automation endeavours as envisioned in air transport, because it includes card counterfeiting, forgery, loss, and theft, frauds that could negatively impede the development of those initiatives.[222] The first one refers to manufacturing, copying or imitating a credit card without the legal right to do so;[223] the second to the "illegal signing, with an intent to defraud, of a credit card or credit card sales slip";[224] and the third to the "illegal acquisition of a credit card belonging to another person".[225] Other types of unauthorised uses of credit or debit cards constitute: 1) fraudulent applications that are issued to criminals; 2) employee fraud whereby an employee provides away sensitive data to criminals; and 3) merchant fraud.[226] As a matter of fact, it has been said that one of the major concerns when developing smart card programmes represents the

---

[218] See A.H Lipis, T.R. Marschall & J.H. Linker, *Electronic Banking* (New York: John Wiley & Sons, 1985) at 51.
[219] See D. O'Mahony, M. Peirce & H. Tewari, *Electronic Payment Systems* (Boston: Artech House, 1997) at 13.
[220] See P. Kirkman, *Electronic Funds Transfer Systems* (Oxford: Basil Blackwell, 1987) at 44.
[221] See D.A. Szwak, "Credit Cards in America" (1995) 13 J. Marshall J. Computer & Info. L. 573 at 577.
[222] See B. Zagaris & S.B. MacDonald, "Money Laundering, Financial Fraud, and Technology: The Perils of an Instantaneous Economy" (1992) 26 GW J. Int'l L. & Econ. 62 at 65 (asserting the negative economic impact of credit card frauds on trading).
[223] See *Black's Law Dictionary, supra* note 147 at 354.
[224] See *Washington (State of)* v. *Jefferson*, 11 Wn. App. 745; 524 P.2d 924 (Wash. 1974).
[225] *Ibid.*
[226] See M.J. Auriemma & R.S. Coley, *Bankcard Business* (Washington: American Bankers Association, 1992) at 141.

formation of a trust-based scheme where customers will fearlessly engage themselves with the system.

In a similar vein, the use of a credit or debit card, as envisioned by the STP initiative, must ensure card bearers the necessary level of consumer protection against any unauthorised use by third persons, since the banking industry has experienced a considerable increase in the number of counterfeit and forged cards.[227] The main problem with such frauds lies in the fact that wrongdoers are able to perform them for long periods of time before being discovered.[228] Debit and particularly credit card frauds usually take a long time to detect.[229] Some commentators have even expressed that the *Financial Privacy Act of 1978*[230] severely hampers the investigation process undertaken to reveal these frauds in the United States, because it limits access to the records by the authorities, who then cannot expeditiously investigate the case.

The development of smart cards will represent a lesser degree of fraud risk because the cards will most likely have a chip, as opposed to a magnetic stripe; the latter is considerably easier to counterfeit without damaging the card. It has been indicated that smart cards offer a securer environment for data contained therein. However, this thesis supports the idea that the credit and debit card experience with unauthorised uses give invaluable tips when dealing with the SPT initiative. Therefore, an assessment of the two main legal instruments addressing the unauthorised use of debit and credit card in the United States becomes necessary.

3.1.3. Regulation E

---

[227] See also D.V. Macdougall, R.G. Mosley & G.J.I. Sanders, *Credit Card Crime in Canada* (Ottawa, Canadian Association of Crown Counsel, 1985) at 2.
[228] See M.E. Matthews, "Credit Cards – Authorised and Unauthorised Use" (1994) 13 Ann. Rev. Banking L. 233.
[229] See B.F. Caminer, "Credit Card Fraud: The Neglected Crime" (1985) 76 J. Crim. L. & Criminology 746 at 748.
[230] See 12 U.S.C. 3405.

The *Electronic Fund Transfer Act of 1978*, designated as Regulation E, was enacted to protect the individual consumer from unauthorised interception of electronic transactions, including debit cards, under its scope of applicability. The regulation obliges the financial institution to disclose the extent of consumer liability for unauthorised electronic transfers.[231] The financial institution is also required to provide a receipt of the electronic transaction as well as a periodic statement.[232] The liability of the consumer is limited to US$ 50 for unauthorised transfer provided the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device,[233] shifting liability to the issuer, who is encouraged to get insurance.[234]

An error resolution procedure enables consumers to give oral or written notice to the financial institution of any discrepancies within 60 days after the financial institution sends the periodic statement or delivers a passbook documentation.[235] Finally, Regulation E grants consumers the right to deny any issuance of unsolicited services provided thereof.[236] Should the SPT system adopt a debit card in the United States, Regulation E would be applicable. It is interesting to see the consumer approach of the regulation since for cases of unauthorised use, it tremendously limits the liability of the cardholder. This consumer-oriented scenario may not be quite the same in developing countries though, where banking institutions have stronger bargaining power than cardholders and these organisations are able to manipulate adhesion contracts governing the legal relationship between the parties. The lack of adequate consumer protection laws might also severely affect the well-being of users.

---

[231] See 12 C.F.R. 205.7.
[232] See 12 C.F.R. 205.9.
[233] See 12 C.F.R. 205.6.
[234] See S.M. O'Connor, "The de Minimis Exemption of Stored Value Cards From Regulation E: An Invitation to Fraud?" (1998) 5 Rich. J.L. & Tech. 6 at 8; M.E. Budnitz, "Stored Value Cards and The Consumer: The Need for Regulation" (1997) 46 Am. U.L. Rev. 1027 at 1045; B.W. Smith & R.J. Wilson, "How Best to Guide the Evolution of Electronic Currency Law" (1997) 46 Am. U.L. Rev. 1105 at 1121.
[235] See 12 C.F.R. 205.11(b) (1996).
[236] See W.A. Effross, "Putting the Cards Before the Purse?: Distinctions, Differences, and Dilemmas in the Regulation of Stored Value Card Systems" (1997) 65 U.MKC L. Rev. 319 at 340.

3.1.4. Regulation Z

On the other hand the *Credit Card Fraud Act*, designated as Regulation Z,[237] regulates the rights and responsibilities of credit card users, protecting consumers against unauthorised uses thereof. This US statute prohibits the use of unauthorised or fraudulent access devices[238]meaning any card, plate code, account number,[239] or other means of account access that can be used alone or in conjunction with another access device to obtain money, goods, services, or other things of value, or that can be used to initiate a transfer of funds.[240] The act provides a rather broad conceptualisation of credit cards and their probable fraudulent uses, which enables the legal system to adapt to emerging technological changes, as is the case of smart cards. The definition is also of paramount significance especially bearing in mind that forgery and counterfeiting can be achieved through numerous methods and mechanisms.[241] The act also limits the liability of the cardholder to US$ 50 for unauthorised transactions. The cardholder has 60 days to file a complaint to the issuing bank once an account statement has been received.[242] The latter has 90 days to respond to the consumer.[243] However, it is mandatory to clarify that for cases of counterfeiting cards, US courts have repeatedly expressed that consumers are not liable, since those fraudulent acts are beyond their control, and consumers do not have any mechanisms to defend themselves.[244] The courts will most likely favour consumers when called upon to decide a case involving counterfeiting through the use of a smart card.

---

[237] See 12 C.F.R. 226.12-226.13 (1997).

[238] The American Courts have noticed that the word "device" is not limited to physical objects. It could be extended to include "any invention or contrivance, as well as any plan". See *Alaska* v. *Morgan*, 985 P.2d 1022 (Alas. App. 1999).

[239]The courts have also pronounced that the credit card number is included in the definition of "credit card". See *Peterson* v. *Arkansas* (*State of*), 326 Ark. 1004, 935 S.W. 2d 266, 267 (Ark. 1996). See also *Kansas (State of)* v. *Howard*, 221 Kan. 51, 557 P.2d 1280 (Kan. 196).

[240] See 18 U.S.C.1029 (a) & (e). The act also provides "a fine of not more than the greater of $ 50,000 or twice the value obtained by the offence or imprisonment for not more than fifteen sanctions or both" when a credit card has been counterfeited. See generally C. A. Bruens, "Melting the Plastic Theories: Advocating the Common Law of Fraud in Credit Card Non-dischargeability Actions under 11 U.S.C 523 (a) (2) (A)" (1997) 50 Vand. L. Rev. 1257.

[241] See R.F. Stankey, "Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers" (1999) 6 CommLaw Conspectus 11 at 14.

[242] See D.M. Mroz, "Credit or Debit? Unauthorised Use and Consumer Liability Under Federal Consumer Protection Legislation" (1999) 19 N. Ill. U. L. Rev. 589. See generally R.L. Field, "The Electronic Future of Cash: Survey: 1996: Survey of the Year's Developments in Electronic Cash Law and The Laws Affecting Electronic Banking in the United States" (1996) 46 Am. U.L. Rev. 967 at 978; C.L Wilson, "Extending Bank Regulation to Electronic Money and Beyond" (1997) 30 Creighton L. Rev. 671 at 681.

[243] Notice that under Regulation E consumers only have 2 days to complain against unauthorised uses.

[244] See Szwak, *supra* note 221 at 581.

3.2. Inadmissible Passengers

It has been said that implementing smart cards with biometric measurement devices to facilitate the flow of air traffic focused on immigration and customs clearance may directly affect the issue of inadmissible passengers, particularly when those endeavours are applied on a larger scale. It is worth mentioning at the outset of this discussion that the current state of the smart card's development is rather selective and it has been targeted at a somewhat elitist group of passengers. The primordial objective of those initiatives is to remove low-risk passengers from torturous queues. Hence, the endeavour lacks an extensive application. The foregoing supports the idea that issues of inadmissible passengers will rarely be a problem during the early stages of implementation, but rather when a larger degree of development is achieved.[245] Furthermore, it has been said that by introducing biometric measurement devices embedded in smart cards, the risk of counterfeiting, forgery, and impostors should be substantially reduced.

According to Annex 9, an inadmissible passenger is "a person who is or will be refused admission to a State by its authorities".[246] Normally the preceding occurs when the passenger does not have proper documentation and where authorities of a particular State determine that the acceptance of such passenger could considerably constitute a risk to their national citizens. The question then arises whether someone is to be held responsible and liable for bringing an inadmissible passenger to the territory of a State that refuses his acceptance. Abeyratne has indicated that Article 13 of the Chicago Convention[247] establishes the obligation of States to comply with the laws and regulations of the Contracting States where passengers, crew, or cargo are either arriving or departing, particularly in relation to immigration, passports, customs, and quarantine.[248] More specifically, Annex 9 provides that air carriers must be very cautious when checking the passenger's documentation at embarkation in order to ensure they hold those required by the State of transit or

---

[245] See R.I.R. Abeyratne, "Emerging trends on arrest and detention of inadmissible passengers at the airport" (1998) VII:II The Bar Association Law Journal 21.
[246] See *Annex 9*, *supra* note 35, definitions at 2.
[247] See *Chicago Convention*, *supra* note 23, Art. 13.
[248] See R.I.R. Abeyratne, "Air Carrier Liability and state Responsibility for the Carriage of Inadmissible Persons and Refugees" (1998) 10:4 Int'l J. Refugee L. 675 at 677.

destination.[249] Should the passenger be found inadmissible due to improper documentation at the point of destination, the air carrier may be subject to economic fines. However, the air carrier can exempt itself if it can prove that all adequate precautions were taken to ensure that the passenger complied with the entry documentary requirements of the receiving State.[250] Hence, the aforesaid supports the argument that an air carrier could be held financially responsible for cases where a passenger carries a smart card as a travel document and he is found inadmissible. Should such situation arise, the Contracting State must seize the travel documents of the "person impersonating the rightful holder of the travel document", in order to later return the aforesaid document to the State named as issuer.[251] Annex 9 mandates that the removing State must issue a covering letter with a photocopy of the seized document attached thereto.[252] For cases where the documents of the inadmissible passenger have been lost or destroyed, Contracting States must accept a letter issued by the receiving State attesting to the circumstances of embarkation and arrival.[253] For the previously described situations, Contracting States ought not to require the "production of the fraudulent, falsified or counterfeit travel document concerned".[254] It is the responsibility of the air carrier to transport the inadmissible passenger back to his original point of embarkation,[255] a legal duty that terminates when the inadmissible passenger is legally admitted for entry into that State.[256]

Some commentators have already mentioned that implementing smart cards as travel documents could trigger the proper application of the aforesaid procedures, especially taking into consideration that the production of a photocopy of the rejected document will not be

---

[249] See *Annex 9*, *supra* note 35, standards 3.39 & 3.40. The language of Annex 9 goes further to suggest that Contracting States and operators enter into Memoranda of Understanding to establish guidelines for mutual co-operation and support in order to counterattack abuses associated with travel document fraud. In this respect, the positioning of "liaison officers" are recommended. See *Annex* 9, *supra* note 35, recommended practices 3.40.1 & 3.40.2.

[250] See *ibid.*, recommended practice 3.41 & 3.43.

[251] See *ibid.*, recommended practice 3.42.

[252] See *ibid.*, recommended standard 3.45. A format for covering letters applicable to the removal of improperly documented passengers is also suggested. See also *Annex 9*, app. 9.

[253] See *ibid.*, recommended standard 3.49.1.

[254] *Ibid.*, standard 3.50.

[255] See *ibid.*, recommended practice 3.44. However, nothing prevents the air carrier from covering the cost of transportation back to the inadmissible passenger's original point of origin. See *Ibid.*, recommended standard 3.48. Similarly, Annex 9 draws special attention to the fact that every precaution must be taken by the Contracting State and the air carrier to ensure that the life of an inadmissible passenger, seeking political asylum, is not threatened by his deportation at the original point of embarkation.

[256] *Ibid.*, standard 3.51.

available.[257] Instead authorities and passengers will only have a computer record generated by the inadmissible smart card. The question then arises as to whether government authorities of the document's issuing State and courts will accept the computer-generated record.[258] Although the latter is beyond the scope of this thesis, it is important to mention that their acceptance and treatment by courts varies tremendously worldwide. The law of evidence was based upon oral tradition, whereby witnesses were called to testify to what they actually had knowledge.[259] Therefore, the advancement of technology would seem to create friction. However, it is safe to assert that the legal framework in developed countries has evolved in such a way to permit their discovery in legal action. For instance, in the United States Rule, 34 of the Federal Rules of Civil Procedure was changed to permit the inclusion of information stored electronically as discoverable.[260] The Rule provides that any party may inspect and copy, any designated documents and compilations from which information can be obtained.[261] Similarly Canada, through the *Personal Information Protection and Electronic Documents Act*,[262] has established that "any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.[263] Unfortunately, a large number of countries are still reluctant to accept computer-generated records in court, thereby constituting a threat to automation endeavours. [264]

3.3. Critical Assessment

The legal issues previously described constitute extremely valuable concerns when developing the system environment of the STP and electronic identity cards. The legal

---

[257] See R.I.R. Abeyratne, "The Automated Screening of Passengers and the Smart Card – Emerging legal Issues" (1998) XXIII:I Air & Sp. L. 3 at 4.
[258] See generally S. Gale, "The Impact of Information Technology Upon Civil Practice and Procedure" in L. Edwards & C. Waelde, eds., *Law & the Internet* (Oxford: Hart Publishing, 1997) at 245.
[259] See C. Tapper, *Computer Law*, 4th ed., (London: Longman, 1989) at 367.
[260] See also J.H.A. Pooley & D.M. Shaw, "The Emerging Law of Computer Networks: Finding out what's there: technical and legal aspect of discovery" (1995) 4 Intell. Prop. L.J. 57 at 68.
[261] See Fed R. Civ. P. 34. See generally R.I.R. Abeyratne, "Some Recent Trends in Evidential Issues on Electronic Data Interchange – The Anglo American Response" (1994) 13:2 Trading L. R. 103; UNCITRAL, "Legal Value of Computer Records" A/CN.9/265, 21/2/1985.
[262] See *Personal Information Protection and Electronic Documents Act, infra* note 463.
[263] *Ibid.*, s. 31.1.
[264] See generally E. Mackaay, D. Poulin & P. Trudel, eds., *The Electronic Superhighway* (London: Kluwer Law International, 1995) at 99.

responses thereto can vary from country to country since there is no clear harmonisation. However, since at present the development of such initiatives only include their immersion in developed markets, the legal framework therein will most likely be ready to properly confront the emerging trends in air transport. Once these initiatives are planned on a larger scale, further legal studies on each particular issue will be required.

Chapter Four

Privacy

The core legal analysis of this thesis constitutes an examination of how implementing automation in facilitation of air transport directly compromises the privacy rights of individuals. A thorough examination will be conducted in order to determine the degree of intrusion that automation will cause to the right of privacy. It is indeed worth mentioning that all the endeavours envisioned to implement automation in air transport as described in this thesis have privacy connotations of different levels.

4.1. The Shifted Paradigm of Privacy. Towards a Traceable Society?

The undisputed presence of technology in almost every facet of today's life has unarguably enhanced a large number of activities not previously affected thereby; at least this is the trend apparently surfacing the developed world's current reality. The advent of the information superhighway and the emergence of automation have inevitably transformed the social environment of individuals, created unexpected business opportunities, reduced operating costs, accelerated transaction times, facilitated accessibility to communications, shortened distances, and removed bureaucratic formalities.[265] Notwithstanding the attractiveness of the foregoing developments and augmentations, technology has also created a further intrusion into the lives of individuals by means of automated mechanisms, devices, features, and procedures. For instance, when a credit card is used, it is possible to track purchases, discovering numerous aspects about that particular individual, including, food inclination, leisure activities, and consumer credit behaviour.[266] Loyalty cards pursue the espousing of the individual with a specific product, eradicating the search for other viable alternatives. Computer records of an air carrier's reservation system can reveal details about the passenger's travel preferences, *inter alia*, seat selection, destination fondness, ticket purchasing dossier, lodging keenness, temporary address and telephone contacts, attendance at theatres and sport activities, and whether the passenger travels alone or with someone

[265] See generally G. Orwell, *Nineteen eighty-four* (Oxford: Clarendon Press, 1984).
[266] For a detailed analysis of the implications of credit cards with respect the right of privacy see S.L. Nock, *The Costs of Privacy* (New York: Aldine De Gryter, 1993) at 43.

else.[267] Thus, government and the entrepreneurial sector create an atmosphere of surveillance where computer devices monitor individuals' most intimate activities and preferences, leading to the formation of a genuine "traceable society".[268]

Moreover, the empowerment of capabilities envisioned for the smart card in the air transport sector with the adoption of a multi-functional approach, providing copious applications, *inter alia*, credit card, travel document identity card, frequent flyer membership card, long distance telephone card, plus the participation of the government to develop the identification card functionality, could tremendously aggravate the already complex environment. In addition, the API, MRTD, and the Electronic European Identity Card initiatives with their possible inclusion of biometric identification mechanisms, complete the labyrinth of obscurity.

The main problem within this context lies in the fact that an enormous amount of personal information to be handled by such balkanised group of players from the public and private sector exacerbates the possibility of "data leaks" in the system, a risk that could have remarkable legal consequences. The discussion undertaken hitherto suggests that these initiatives may directly impinge upon one of mankind's most precious freedoms: *The Right of Privacy*.

The foregoing sustains the compulsory need for a review of the privacy laws, which may be directly affected by the implementation of such endeavours, in order to assess

---

[267] The paramount importance of airline computer reservation system records can certainly be appreciated in the world-renowned cases *Libyan Arab Jamahiriya* v. *United Kingdom* and *Libyan Arab Jamahiriya* v. *United States of America* regarding the outrageous PAM 103 accident at Lockerbie, Scotland in 1988, where the International Court of Justice requested air carriers to summit to the Court the defendants' flight information and reservation details. See International Court of Justice, News Release 99/36, "Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie" (1 July 1999), online: http://www.icj-cij.org/icjwww/idocket/iluk/iluk2frame.html (date accessed: 14 July 2000). In a similar vein, Arthur R. Miller describes the significance of airline computer reservation system records when dealing with federal, state, local, and other types of investigations where these dossiers could provide valuable information. See also A.R. Miller, *The Assault on Privacy* (Ann Arbor, Michigan: The University of Michigan Press, 1971) at 42.

[268] See G.G. Scott, *Mind Your Own Business – The Battle for Personal Privacy* (New York: Insight Books, 1995) at 307; D. Burnham, *The Rise of the Computer State* (New York: Random House, 1983) at 20. *A contrario* to the argument supported in this thesis that the advancement of technology directly affects the intimacy of individuals, US Circuit Judge Richard Posner favours the idea that other factors, such as urbanisation, income, and mobility development have particularly weakened the information control that,

whether a co-existence of industry trends with the safeguarding of individual's right of privacy is possible. Then, this thesis will proceed to comprehensively examine the right of privacy, describing its recognition in international instruments and highlighting its definition,[269] to later focus primarily on the developments taking place within the European Union, the United States, and Canada, mainly because the air transport industry has been exceptionally keen on developing new initiatives in these particular markets. Special consideration will be given to the legal implications of transborder data flows. Finally, a conclusion will be established, appraising whether the existing worldwide legal framework for privacy laws is adequate to cope with the emerging industry trends, or whether further regulations are needed to comply with the Roman principle *"De Lege Ferenda"*.

4.2. The International Recognition of the Right of Privacy

Privacy was first recognised as a fundamental freedom in the Universal Declaration of Human Rights.[270] Thereafter, several other human rights conventions followed the same trend, granting to individuals the fundamental right of privacy.[271] The primordial concern of these international instruments was to establish the necessary legal framework to protect elementary rights, focusing essentially on the individual *per se*.

4.2.1. OECD Guidelines

Later, in the early 1980's the Council of the Organisation for Economic Co-operation and Development (OECD) witnessed a reduced flow of information, which could

---

for instance, the government has over individuals; this denotes that individuals' privacy has increased. See R. Posner, "The Right of Privacy" (1978) 12:3 Ga. L. Rev. 393 at 409. [hereinafter *Posner*]

[269] Although an effort to conceptualise privacy will be attempted, this thesis understands the risk of establishing narrow definitions that do not suffice to cover the myriad of possible issues that may arise, a concern already established in the roman principle: *"Omnis definition in jure civili periculosa est, parum est enim ut non subverti possit."* See *Black's Law Dictionary, supra* note 147 at 1671.

[270] The text reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". See *Universal Declaration of Human Rights*, GA Res. 217(III), 10 December 1948, art.12.

[271] See *International Covenant on Civil and Political Rights*, GA Res. 2200 (XXI), 16 December 1966, art. 17; *American Declaration on the Rights and Duties of the Man* (1948), art. 5; *American Convention on Human Rights*, 22 November 1969, San Jose, Costa Rica, art. 11; *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S.5, art. 8; *United Nations Convention on Migrant Workers*, A/RES/45/158, 25 February 1991, art. 14; *United Nations Convention on Protection of the Child*, GA Res. 44/25, 12 December 1989, art.16.

ultimately have caused a serious disruption in important sectors of the global economy.[272] Hence, recommendations as to voluntary non-binding guidelines governing the protection of data privacy and transborder flows were formulated, seeking to protect the economic interests of its members.[273] The original interest in granting the right of privacy to the individual was slightly shifted towards an economic approach to the issue, particularly taking into consideration the advancement of technology. Thus, the guidelines originally attempted to create a somewhat harmonised environment for the protection of privacy data, discouraging restrictions on flows between members thereof.[274] The *rationale* was that if all the members had the same standard and level of protection, there would not be any apprehension of transmitting data, hence, there would not be any restrictions on the flows.[275] The OECD guidelines address eight major principles: 1) the data should be collected and obtained lawfully and fairly; 2) the data should be relevant to their purposes, embedding the data quality principle; 3) the data should be specifically collected to serve their intended purposes, and further eliminated if no longer needed; 4) the data should be used solely for the purposes originally intended; 5) the data should be handled in secure environments; 6) the data should be available to persons making inquiries; 7) the data subject should have the right to access and challenge the information; and 8) the data should be administered by a designated controller in charge of giving effect to these guidelines.[276]

4.2.2. United Nations Guidelines

Similarly, the United Nations also understood the problems caused by the development of technological devices, essentially that would be used to store files and that they would have possible implications for the right of privacy.[277] Thus, in 1990 the United

---

[272] See C. Martin, "Mailing List, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem" (1998) 35 Hous. L. Rev. 801 at 807.

[273] See OECD, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc. No. OECDC 58 Final (1980) [hereinafter *OECD Guidelines*]. Although never adopted, the United States signed the OECD Recommendations.

[274] See generally OECD, *Information, Computer, Communication Policy* (Paris: OECD, 1983)

[275] See P.A. Monahan, "Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses" (1998) 29 Law & Pol'y Int'l Bus. 275 at 284.

[276] See Justice M. Kirby, "Legal Aspects of Transborder Data Flows" (1991) 9 Computer L.J. 233 at 238.

[277] See generally J. Michael, *Privacy and Human Rights* (Hampshire, England: Dartmouth Publishing Company, 1994) at 19.

Nations established the "Guidelines Concerning Computerised Personal Data Files",[278] which were originally based on a draft prepared by the General Assembly of the Commission on Human Rights.[279] The Guidelines were conceived as a model for enactment of national laws, as well as their adoption by international agencies.[280] The primordial focus of these Guidelines was shifted back to the human rights of the individual and the technological encroachment implications thereof, *vis-à-vis* the economic interest pursued by the OECD Guidelines.[281]

Even with such international acknowledgement of the right of privacy, conceptualisation becomes a rather difficult task due to the disparity of approaches thereto, which comprises several fields of studies, not just solely within the sphere of law. Privacy denotes philosophical connotations with possible legal implications, but yet the term has not been defined.[282]

4.3. The Concept of Privacy

One of the main problems when defining privacy is that its connotation represents different things for different people.[283] The concept *per se* has evolved throughout the history of mankind, from the original non-intrusion approach, which defended an individual's property and physical body against unwanted invasions and intrusions, then manifesting in whom to associate with, later enlarging its scope to include privacy as the individual's decision-making right,[284] and culminating in the control over one's personal information.[285]

---

[278] See *Guidelines for the regulation of computerised personal data files*, GA Res. 45/95, 68th Plenary Sess. (14 December 1990).
[279] See *Draft Guidelines for the regulation of computerised personal data files*, GA Res. 1989/44, 44th Sess. (15 December 1989).
[280] See I.J. Lloyd, "Data Protection" in C. Redd, ed., *Computer Law* (London: Blackstone Press Limited, 1996) 325 at 332.
[281] For a chronological international evolution of the new laws on computers and personal privacy, see M.R. Rubin, *Private Rights, Public Wrongs* (New Jersey: Able Publishing, 1988) at 87.
[282] The former Privacy Commissioner of British Columbia, Canada, has asserted that privacy was originally a "non-legal concept". See D.H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection" (1991) 41 Case W. Res. 831 at 833.
[283] See P.M. Regan, *Legislating Privacy* (Chapel Hill, North Carolina: The University of North Carolina Press, 1995) at 33; P.A. Freund, "Privacy: One Concept or Many" in J.R. Pennnock & J.W. Chapman, eds., *Privacy* (New York: Atherton Press, 1971) at 182.
[284] See *Roe v. Wade*, *infra* note 311. See also Cate, *infra* note 300 at 61.
[285] See *German case*, *infra* note 292. See also S. Hoffer, *World Cyberspace Law* (Juris Publishing, 2000) at 8.1; R. Gavison, "Privacy and the Limits of the Law" (1980) 89 Yale L.J. 421.

Thus, the conceptual evolution of privacy is directly related to the technological advancement of each particular period in history.

In the United States Judge Thomas M. Cooley enounced the concept that privacy is the right "to be let alone" as a part of a more general right to one's personality.[286] This idea was mentioned in the seminal article "The Right of Privacy" written by two prominent young lawyers, Samuel D. Warren and Louis D. Brandeis[287], in 1890.[288] The *rationale* of the notorious article attempted to denounce the outrageous intrusion of the Bostonian yellow press into the individual's private affairs. Hitherto, the concept of privacy relied primarily on a somewhat physical and territorial understanding, the protection against invasions on the individual's private property or life. Later, Alan Westin pronounced the foundations for the conceptualisation of "the information privacy", whereby the individuals would determine when, how, and to what extent information about themselves would be communicated to others, thus creating the concept of the control of information about oneself.[289] With the development of computer capabilities to handle large amounts of data, privacy has been enlarged to include the collection, storage, use, and disclosure of personal information.[290] The notion of informational privacy protection has been particularly adopted in the United States, as opposed to the term "data protection" used in Europe.[291]

---

[286] See T.M. Cooley, *A Treatise on the Law of Torts*, 2nd ed. (Chicago: Callaghan, 1888), as cited in S.D. Warren & L.D. Brandeis, "The Right of Privacy" (1890) 4:5 Harv. L. Rev. 193 at 195.

[287] Louis D. Brandeis later became a notorious US Supreme Court judge.

[288] Although the definition of privacy as the "Right to be Alone" is often erroneously attributed to Warren and Brandeis. See Warren & Brandeis, *supra* note 286 at 195. Additionally the concept of privacy as "the right to be let alone", and as "the right most valued by civilised man" was embraced by US courts in the landmark dissenting opinion of Justice Louis D. Brandeis in *Olmsted* v. *United States*. See *Olmsted*, *infra* note 317.

[289] See A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 368. For a similar conceptualisation of privacy, see C. Fried, "Privacy: Economics and Ethics A Comment on Posner" (1978) 12 Ga. L.Rev. 423 at 425.

[290] See J.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. 497 at 498.

[291] See Flaherty, *supra* note 282 at 834. The term "data protection" has been translated from the German word *Datenschutz*, referring to a set of policies seeking to regulate the collection, storage, use, and transfer of personal information. See C.J. Bennet, *Regulating Privacy* (Ithaca, New York: Cornell University Press, 1992) at 13.

The idea of privacy self-determination was first judicially embraced by the German Bundesverfassungsgericht in 1983.[292] Subsequently, the US Supreme Court followed the trend by adopting the principle in *DOJ* v. *Reporters Comm. for Freedom of the Press*.[293] Hence, bearing in mind that all the endeavours and initiatives undertaken to implement automation mechanisms to facilitate the flow of traffic in air transport involve the processing of personal data for the objectives pursued thereof, this thesis sustains that although there may be a large number of valuable definitions and approaches to privacy, for the purposes of this research the self-determination conceptualisation herein exposed suits it most adequately.[294]

Nevertheless, privacy is not an absolute, unlimited right that lives in isolation.[295] Hence, there is frequently the necessity to balance the former with other conflictive rights, such as the freedom of speech and the right to access information, an equilibrium that is also sought when examining individuals' rights *vis-à-vis* the interest of society.[296] Hence, when called to resolve privacy matters, the courts will most likely favour the application of a balance test to the issue at bar, especially if the government is involved therein.

4.4. Privacy in the United States

The right of privacy originally evolved in the United States following the appearance of the influential article written by Warren and Brandeis. This legal response stemmed from the increasing intrusion of the newspaper media, particularly the yellow press, which publicly

---

[292] In a remarkable case concerning the legality of a national census scheduled by the authorities, the German Constitutional court connected the individual's liberty and the personal data processing of the intended census, to rule that if the individuals do not know for what purposes and who is collecting the data, that situation will eventually create an abdication of the individual's rights to the processor's command, "which cannot be tolerated in a democratic society". See S. Simitis, "From the Market to the Polis: The EC Directive on the protection for Personal Data" (1995) 80 Iowa L. Rev. 445 at 447-448.

[293] See *DOJ* v. *Reporters Comm. for Freedom of the Press*, 489 U.S. 749 at 763 (1988).

[294] Although informational privacy constitutes a major concern when dealing with the processing of data in the automation endeavours undertaken in air transport, physical privacy also denotes significance, particularly when dealing with the inclusion of biometric measurement features, as shown herein later.

[295] See A. Simmel, "Privacy Is Not an Isolated Freedom" in J.R. Pennnock & J.W. Chapman, eds., *Privacy* (New York: Atherton Press, 1971) at.71.

[296] See A. Halpin, *Rights & Law Analysis & Theory* (Oxford: Hart Publishing, 1997) at 111. See also L.G. Foschio, "Motor Vehicle Records: Balancing Individual Privacy and the Public's Legitimate Need to Know" in T.R. Kuferman, ed., *Privacy and Publicity* (London: Meckler, 1990) at 35. For a comprehensive study on the conflictive interest on privacy and the mass media and the Freedom of Speech, see D.R. Pember, *Privacy and the Press* (Seattle: University of Washington Press, 1972) at 227; J.B. Prowda, "A Layer's Ramble Down the Information Superhighway: Privacy and Security of Data" (1995) 64 Fordham L.

scrutinised personal issues of the Bostonian society in the late 1800's.[297] Although the decisive article stresses the importance of protecting the individual right of privacy against the mass media invasion thereto by suggesting that an independent cause of action under tort law is necessitated, the issue lies merely within the sphere of private individuals.[298]

Therefore, it is indeed mandatory to differentiate the possible scenarios when addressing issues of privacy rights. The United States has a two-fold approach to the right of privacy: 1) The Public Sphere: between the individual and the State; and 2) The Private Sphere: between individuals themselves. The former comprises part of US Constitutional law, since indirect references to privacy are enclosed in the Bill of Rights, constituting a federal matter, and some specific legislation Congress has enacted therefore.[299] The latter is covered through the law of torts, and is hence a state matter, and specific legislation regulating certain industries.[300] It should be noted that the United States, faithful to its capitalism principles, has adopted the approach of sectoral regulation in terms of privacy, as opposed to the enactment of "omnibus data protection statues" undertaken in Europe.[301] Thus, the US conceptualisation of privacy supports as little government interference as possible, inasmuch as the market will regulate itself. The *rationale* of the foregoing discussion lies in three facts. Firstly, a large number of Americans believe that their rights can be adequately protected through the implementation of industry codes, norms and business practices, company policies, proper technical network structure, good corporate citizenship through the implementation of guidelines,[302] and perhaps even through contractual arrangements, meaning that the market has matured sufficiently enough to be self-

---

Rev. 738 at 769. See also J. Montgomery Curtis Memorial Seminar, *The Public, Privacy and the Press: Have the Media Gone Too Far?* (American Press Institute, 1992) at 2.

[297] Apparently the concern of Samuel Warren for privacy was borne when his wife's entertainment activities were scandalised by the emerging Bostonian yellow press. See Miller, *supra* note 267 at 170. For a good study on colonial privacy in New England, see generally D.H. Flaherty, *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1972) at 164.

[298] See Flaherty, *supra* note 282 at 835.

[299] The US Supreme Court has strongly affirmed that the US Constitution does not grant privacy rights to private individuals among themselves, thus leading to its resolution to the law of torts. See *Prudential Insurance Co.* v. *Cheek*, 259 U.S. 530 at 543 (1922).

[300] See F.H. Cate, *Privacy in the Information Age* (Washington, DC: Brookings Institution Press, 1997) at 49. See also W. Zelermyer, *Invasion of Privacy* (Syracuse: Syracuse University Press, 1959) at 16.

[301] See I.J. Lloyd, *Information Technology Law* (London: Butterworths, 1997) at 38.

[302] For an interesting business guidelines compromise with respect to the privacy of customers, see Direct Marketing Association, "Privacy Promise Member Compliance Guide - Keeping Our Privacy Promise to Consumers" online: http://www.the-dma.org/library/privacy/privacypromise.shtml (date accessed: 13 July 2000).

regulated.[303] It reflects the trust of the American people in the private sector. *A contrario*, numerous commentators and predominantly civil liberties groups have expressed profound concerns about whether further government intervention has become mandatory.[304] Secondly, the tremendous power of influential industry lobbying groups strongly oppose any further government intervention with business. As opposed to their European counterparts, who are extremely keen on striking when the government does not grant them what they want, these US lobbying groups have direct access to the White House, hence representing considerably more bargaining power than the individual data subject.[305] Thirdly, the United States favours the free flow of information according to the principles embraced by the First Amendment,[306] based on the premise that the availability of information will be regulated by marketplace ideas, hence reflecting an enormous trust thereto.[307] In addition, some commentators, such as Richard Posner, suggest that an excessive protection of personal information would inevitably distort efficient market functions.[308] Therefore, it is unlikely that the US Congress will enact a general comprehensive set of rules addressing privacy, as contained in the European spectrum.[309]

4.4.1. Privacy Dimensions

---

[303] See Reinberger, *supra* note 290 at 515.

[304] See J.R. Reidenberg, "Restoring Americans' Privacy in Electronic Commerce" (1999) 14 Berkely Tech. L.J. 771 at 792; R. M. Gellman, "Fragment, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions" (1993) 6 Software L.J. 199; M.E. Budnitz, "Privacy Protection for Consumer Transactions in Electronic Commerce" Why Self-Regulation is Inadequate" (1998) 49 South Carolina L. Rev. 847 at 860 (expressing that although acknowledging the serious threats to the privacy of consumers, the US Government has decided to adopt an industry self regulation approach conflicting with the EC Directive); P. Mell, "A Hitchhiker's Guide To Trans-Border Data Exchanges Between EU Member States and the United States under the European Union Directive on the Protection of Personal Information" (1991) 9 Pace Int'l L. Rev. 147 at.182; J.M. Myers, "Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain and the United States" (1997) 29 Case W. Res. J. Int'l L. 109 at 146.

[305] See generally J. Rule et al., *The Politics of Privacy* (New York: Elsevier, 1980).

[306] United States, Constitution, amendment first.

[307] With this respect, Fred H. Cate has written:

> the U.S. approach to information privacy inevitably results in some harm to individual's privacy, reputations, and sensibilities, but it reflects a constitutional calculation that such harm is less threatening to the body politic than the harm associated with centralised privacy protection, government interference with the information flows necessary to sustain democracies and markets, and the growing ineffectiveness of omnibus legal controls in the face of the widespread proliferation of powerful information technologies.

F.H. Cate, "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33 Ind. L. Rev. 174 at 231.

[308] See Posner, *supra* note 268 at 400.

Commentators in the United States have been fond of establishing five dimensions or categories of privacy: "Physical Privacy" would be addressed through issues related to the physical integrity of the individual, originally protected through the tort of trespass to the person.[310] Secondly, "Decisional Privacy", embraced in the landmark *Roe* v. *Wade*,[311] where the US Supreme Court extended the right of privacy to make one's own decisions to activities related to marriage, procreation, contraception, abortion, family relationships, and education. Thirdly, "Communications Privacy", related to the First Amendment's Freedom of Speech and Association, whereby an individual is granted the right to freely communicate among peers. Fourthly, "Territorial Privacy" seeks to set limits or boundaries on intrusion into a specific space or area in one's property. Fifthly, "Information Privacy" tackles the control of handling of personal data.[312] This thesis will primarily focus on the latter, since is clearly more related to the problems discussed herein.

The initiatives and endeavours envisioned to implement facilitation in air transport by means of automation will undoubtedly trigger both the public and private spheres of privacy laws in the United States, mainly because of the amount of personal data to be handled and the participation of the government in most of the aforesaid initiatives. Consequently, the next section of this chapter will thoroughly analyse them both.

4.4.2. Public Sphere of US Privacy Laws

Nowhere in the US Constitution is there any direct reference to privacy; however, the Bill of Rights addresses it indirectly, hence the First Amendment rights of Freedom of

---

[309] See P. Samuelson, "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy", Book Review of *Data Privacy Law, Study of United States Data Protection* by P.M Schwartz & J.R. Reidemberg (1999) 87 Cal. L. Rev. 751 at 763.

[310] Originally the law solely provided a remedy for physical interference with the life and property of the individual. See M.L. Erns & A.U. Schwartz, *Privacy - The Right to Be Let Alone* (New York: McMillan, 1962) at 47.

[311] In this case, the US Supreme Court acknowledged the right of women to have abortions based on the grounds that the federal government could not interfere within her "decisional privacy" sphere. See *Roe* v. *Wade*, 410 U.S. 113 (1973).

[312] See D.R. Tan, "Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union" (1999) 21 Loy. L.A. Int'l & Comp. L.J. 661 at 664.

Speech, Press and Association,[313] the Third Amendment,[314] relating to the quartering of soldiers, the Fourth Amendment right to be free from unreasonable searches,[315] and the Fourteenth Amendment containing the due process clause.[316] Most constitutional issues related to privacy have been dealt with through the Fourth Amendment. Nevertheless, the inception of privacy rights in US Constitutional law was somewhat late, which is surprising for a nation so fond of protecting civil liberties. It was only with the illustrious dissenting opinion of Justice Louis Brandeis in *Olmstead* v. *United States*[317] that the constitutional right of the individual's privacy was conceived.[318] Brandeis pursued to establish the legal ground for protection of the right of privacy against the unlawful intrusion of the government into one's personal affairs. However, in *Olmstead* v. *United States*[319] the US Supreme Court upheld the ruling of the Circuit Court of Appeals for the Ninth Circuit, whereby obtaining evidence without physically invading constitutionally protected areas of the speaker, in this case wiretapping, did not constitute a violation of the Fourth Amendment; hence, it did not constitute an illegal search. The court's decision created the physical invasion requisite, adopting the so-called trespass theory of searches and seizures of tangible property, thereby enlarging the scope of government intrusion in the individual's private life.[320] The first federal constitutional case where the right of privacy was officially recognised by the US Supreme Court was *Griswold* v. *Connecticut*,[321] where Justice Douglas delivering the majority

---

[313] See United States, *Constitution*, amendment 1.

[314] See *ibid.*, amendment 3.

[315] At the outset, the Fourth Amendment was envisaged as a safeguard to protect private property interests against the abuse of the federal government, a situation that was frequent during colonial times. The concept was later extended to include privacy. See D.E. Lively, *Landmark Supreme Court Cases* (Wesport, Connecticut: Greenwood Press, 1999) at 277. The full text of the amendment reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

United States, *Constitution*, amendment 4.

[316] See *ibid.*, amendment 14.

[317] See *Olmstead* v. *United States*, 277 U.S. 438, 478 (1928) [hereinafter *Olmstead*].

[318] See B. Schwartz, *A Commentary on the Constitution of the United States*, vol. I (New York: McMillan Company, 1968) at 171.

[319] See *Olmstead*, *supra* note 317. The same *rationale* was later adopted in *Goldman* v. *United States*, 316 U.S. 129 (1942).

[320] *Olmstead*, *ibid.* included the secret activities of alcohol smugglers, who were intercepted by the police. The ruling of the court came when the prohibition of alcohol was at its peak. Due to the fact that the smuggling of alcohol became a major concern for the US authorities and the media itself, it is likely that the court was influenced by those factors.

[321] See *Griswold* v. *Connecticut* 381 U.S. 479 (1965) [hereinafter *Griswold*]. The case involved the claim of a couple against a statute of the State of Connecticut prohibiting the giving of contraceptive information. The court ruled in favoured of the couple, granting the "marital right of privacy"; however, the court failed

opinion of the court, said that "specific guarantees of the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance... Various guarantees create zones of privacy".[322] The opinion of Justice Douglas acknowledged the protection of privacy contained in the Bill of Rights, inferring the applicability of the First, Third, Fourth, Fifth, and Ninth Amendments thereto. The fundamental value of this case lies in the recognition of the court that several parts of the US Bill of Rights indirectly refer to and thus protect the right of privacy. Subsequently, *contrario sensu* to its original ruling in *Olmstead*, the US Supreme Court in the landmark case *Katz* v. *United States*[323] adopted a broader interpretation of the protection of privacy rights, stating that the Fourth Amendment protects people rather than zones or areas of privacy, leaving behind the "trespass" tangible requirement previously adopted in *Olmstead*.[324]

Thereafter, in *Smith* v. *Maryland*[325] the US Supreme Court was questioned whether the installation of a pen register tape[326] at a telephone company upon police request, to listen to phone conversation of a presumed robber, constituted a search requiring a warrant under the Fourth Amendment. In an interesting decision the US Supreme Court held that when the data subject does not have a "legitimate expectation of privacy", the installation of such pen register tape for the purpose of monitoring calls does not constitute a search. The Court, in order to deal with constitutional privacy issues, established the "legitimate expectation of privacy test" comprising a two-fold requirement. First, the Court analysed whether the individual had a legitimate expectation of privacy. If so, the Court proceeded to examine whether society is prepared to recognise that expectation as reasonable, and whether the individual is entitled to be free from unreasonable governmental intrusion. Similarly, Justice

---

to define such a right. See W. Page Keeton, ed., *Prosser and Keeton on Torts*, 5th ed. (St. Paul, Minnesota: West Publishing, 1984) at 867.

[322] *Griswold*, *ibid.* at 484. The principle of constitutionally protected areas of privacy was adopted, *inter alia*, in *Silverman* v. *United States*, 365 U.S. 505 (1961); *Lopez* v. *United States*, 373 U.S. 427 (1963); *Berger* v. *New York*, 388 U.S. 41 (1967).

[323] See *Katz* v. *United States*, 389 U.S. 347 (1967). The same *rationale* was adopted by the US Supreme Court in *Terry* v. *Ohio*, 392 U.S. 1 at 9 (1968).

[324] The case involved the wiretapping of a telephone conversation that an individual conducted from a public telephone booth, where a recording device was attached. See also C.J. Antieau, *Modern Constitutional Law*, vol. I (San Francisco: Brancroft Whitney Company, 1969) at 160.

[325] See *Smith* v. *Maryland (State of)*, 442 U.S. 735 (1979). The same reasoning was held in *Bond* v. *United States*, 120 S. Ct. 1462 (2000) [hereinafter *Bond*] and *California (State of)* v. *Ciraolo*, 476 U.S. 207 (1986).

[326] A pen register tape was later defined as "a device which records or decodes electronic or other impulses which identity the numbers dialled or otherwise transmitted on the telephone line to which such device is attached". See 18 U.S.C. § 3127 (3) (1994).

Breyer in his dissenting opinion in *Bond* v. *United States*[327] expressed his deep concern about the fact that the "actual expectation of privacy" is of a subjective matter, but its determination must be "objectively" reasonable.[328] It is indeed interesting that the "legitimate expectation of privacy test" established in *Smith* v. *Maryland* places a considerable onerous burden on the individual, who must prove not only infringement of a right, but also the reasonableness of his "legitimate expectation" thereto. Additionally, the second component of the aforesaid test confers a significant discretionary spectrum of decision making to the Courts on a case-by-case basis. Thus, one can question inasmuch as the hurdles envisioned herein, the level of privacy protection given to the data subject by this precedent, which has recently been followed by lower courts in the United States.[329]

Hitherto, all the cases examined herein dealt with general issues of privacy protection in US courts, but with no direct reference to the implementation of automation devices to collect personal data, as is the case this study pursues. Therefore, in *Whalen* v. *Roe*[330] the US Supreme Court was questioned whether the State of New York may record in a centralised computer file the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and unlawful market. The Court held in favour of the State of New York that there was no invasion of privacy, and that the State does have the right to collect such data for public purposes. By indeed establishing its legality, this particular case has enormous relevance to the processing of personal data by the State or any government agency.[331]

A strong argument against giving further personal information to the government when requested to comply with duties and transactions is supported in the belief that by doing so, the individual's control of privacy decreases,[332] allowing undesired governmental

---

[327] See *Bond*, *supra* note 325.
[328] See J.H. F. Shattuck, *Rights of Privacy* (Skokie, Illinois: National Textbook Company, 1977) at 19.
[329] See *Bond*, *supra* note 325. Furthermore, in *U.S.* v. *Smith*, 91-5077 (5th Cir. 1992), involving a case of interception of cordless phone conversation, the claim was denied on the basis that the plaintiff failed to introduce evidence that his subjective expectation of privacy was reasonable.
[330] See *Whalen* v. *Roe*, 429 U.S. 589 (1977).
[331] See generally A.M. Jurevic, "When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail" (1998) 66 Univ. of Missouri at Kansas City L. Rev. 809.
[332] See generally D.H. Flaherty, *Privacy and Government Data Banks* (London: Mansell, 1979) at 19.

surveillance thereof.[333] The aforesaid idea was experienced when in 1934 US President Franklin D. Roosevelt signed the Social Security Act[334] as part of the his "New Deal" programme.[335] A large number of individuals believed that the registration form was a direct invasion of privacy, which was aggravated by the fact that the Social Insurance Number was required to perform numerous regular activities.[336]

One can rightly elaborate a hypothetical case whereby a US INSPASS user refuses to give personal data to the proper government agency on the basis that such collection of information represents an infringement of the right of privacy, as protected by the Fourth Amendment. Following the *rationale* held in *Whalen* v. *Roe*, one could argue that US courts tend to favour government agencies when collecting personal data from individuals in order to comply with the programme's objectives, as long as they pursue a public purpose, such as the one sought by implementing the US INSPASS programme. Hence, the user's claim would be denied.

In a similar vein, the US INSPASS programme conceives the idea of biometric measurement devices embedded in smart cards, specifically hand geometry, with direct application in air transport. Some commentators have asserted that when the government requires citizens to summit biometric identity information, it directly affects physical and informational privacy.[337] Thus, this thesis will proceed to analyse whether the governmental requirement of complying with the hand geometry process may constitute an unreasonable search and seizure under the protection of the Fourth Amendment, creating an invasion of the individual's privacy.

---

[333] See also L. Harris & A.F. Westin, *The Dimensions of Privacy* (New York: Garland Publishing, 1981) at 66.
[334] See *Social Security Act*, 42 U.S.C. 301-1011.
[335] See Killerlane, *supra* note 180 at 1349.
[336] Accordingly, US courts have held consistency the right of the government to require the Social Security Number. See *Arthur* v. *Department of Soc. & Health Servs.*, 576 P.2d 921 (Wash. Ct. App. 1978); *Chambers* v. *Klein*, 564 F. 2d 89 (3d Cir. 1977); *Conant* v. *Hill*, 326 F. Supp. 25 (E.D. Va. 1971), as cited in Killemane, *ibid.* at 1350.
[337] See J.D. Woodward, *supra* note 173 at 99.

In *Iacobucci* v. *Newport*[338] the US Court of Appeals for the Sixth Circuit held the right of the City of Newport to request compliance with the fingerprinting ordinance for all bar employees. Accordingly, in *Perkey* v. *Department of Motor Vehicles*[339] the Californian court was in favour of asserting the right of the state to require individual citizens to provide fingerprints prior to obtaining a license. In *Skinner* v. *Railway Labour Executives Association*,[340] the US Supreme Court acknowledged that a State Regulation compelling the collection and testing of railway employees' urine constituted a "search subject to the demands of the Fourth Amendment"; however, applying the public interest test to the case in question, the US Supreme Court considered that the State Regulation sought to achieve public safety for the benefit of society, which indeed outweighed the individual's expectation of privacy. Then, in *Vernonia* v. *Wanye Acton*[341] the US Supreme Court held that a school district's policy authorising drug testing of students participating in the district's athletics programmes did not violate the Fourth Amendment because the public interest was best served thereby.[342]

The foregoing cases clearly support the argument that US courts, within the public sphere of the constitutional right of privacy, show a tendency to establish the two-fold test conceived in *Smith* v. *Maryland*, whereby the individual's expectation of privacy is balanced against the public interest of society. Therefore, this thesis sustains that when a federal agency seeks to implement automated devices such as biometric measurement embedded in a smart card with the purpose of accelerating the passenger traffic flows, rarely will US courts find a situation where a privacy right under the protection of the Fourth Amendment has been violated, because the public interest is best served. The US constitutional public sphere of privacy protection seems not to need any major amendments to cope with this type of technological advancement.[343]

---

[338] See *Iacobucci* v. *Newport (City of)*, 785 F.2d 1354 (6th Cir. 1986). Similar decisions were previously given in *Thom* v. *New York Stock Exchange*, 306 F. Supp. 1002 (S.D.N.Y. 1969); *Miller* v. *New York Stock Exchange*, 425 F.2d 1074 (2d Cir. 1970).

[339] See *Perkey* v. *Department of Motor Vehicles*, 42 Cal. 3d 185 (1986).

[340] See *Skinner* v. *Railway Labour Executives Association*, 489 U.S. 602 (1989).

[341] See *Vernonia* v. *Wanye Acton*, 513 U.S. 1145 (1995).

[342] For a comprehensive examination of the conflictive interest between privacy and public safety in drug testing cases, see J. Wagner Decew, *In Pursuit of Privacy* (Ithaca, New York: Cornell University Press, 1997) at 125.

[343] See J.D. Woodward, Jr, Biometrics; Identifying Law & Policy Concerns" in A. Jain, R. Bolle & S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (Boston: Kluwer Academic Publishers, 1999) at 403.

4.4.2.1. United States Federal Statutes

Additionally, the United States has enacted the *Freedom of Information Act of 1967* (FOIA),[344] whose main purpose is to provide citizens with the right of access to governmental information, thereby granting full agency disclosure, unless the information is exempt under the provisions thereof.[345] It is noteworthy that the FOIA is not applicable to private individuals.[346] Later the United States enacted the *Privacy Act of 1974*,[347] which seeks to achieve five main objectives: 1) to determine what records the federal agency has on a particular individual; 2) to prevent the misuse of such records; 3) to enable individuals to correct such records; 4) to establish a duty of care in collecting and maintaining information about the data subject; and 5) to hold the agency liable for damages in case of infringement of the act. The act limits the type of personal information federal agencies may store.[348] The significance of the FOIA lies in the fact that in implementing automation devices as envisioned in air transport, it provides accessibility of the data subject to the information obtained by government agencies; such is the case of the US Immigration and Naturalisation Service for the purpose of the INSPASS programme. For instance, one can foresee an INSPASS user requesting access to records contained therein, since the US legal framework provides such a right. Similarly, the Privacy Act grants to the American data subject a longed for "Bill of Rights", creating the necessary legal framework to regulate the activities between

---

[344] See 5 U.S.C. 552 (1994).

[345] There are nine exemptions dealing with issues, *inter alia*, national security information, internal agency material with no public interest, trade secrets and confidential business information given to the agency from outside the government, investigatory records compiled for law enforcement purposes, and internal communications within the executive branch. See J.D. Franklin & R.E. Bouchard, eds., *Guidebook to the Freedom of Information and Privacy Acts*, vol. 1, 2nd ed. (New York: Clark Boardman Callaghan, 1995) at 1-11. See also B.A. Braverman & F.J. Chetwynd, *Information Law*, vol.1 (New York: Practising Law Institute, 1985) at 12.

[346] In *DOJ* v. *Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), the US Supreme Court clarified that the main purpose of the FOIA was to ensure that the activities of the federal government be opened to public scrutiny, but not information about private citizens that happens to be stored in the federal government's warehouse, thereby limiting the access to third parties. See also W.L. Casey, Jr., J.E. Marthinsen & L.S. Moss, *Entrepreneurship, Productivity, and the Freedom of Information Act* (Lexington, Massachusetts: Lexington Books, 1983) at 11.

[347] See 5 U.S.C. § 552a.

[348] See Braverman & Chetwynd, *supra* note 345 at 778. The courts have established that the purpose of the Privacy Act is to protect the privacy of individuals' records in computerised information systems maintained by the federal government. See *Thomas* v. *United States Dept. of Energy*, 719 F.2d 342 (1983); *Kimberlin* v. *United States Dept. of Justice*, 788 F.2d 434 (CA7 111, 1986); *Vymetalik* v. *FBI*, 251 App DC 402 (1986); *Voelker* v. *Internal Revenue Service*, 489 F. Supp. 40 (ED Mo., 1980).

private individuals and the government agencies.[349] Needless to say, the Privacy Act creates a cause of action in favour of the individual when the government agency, such as US INS, mishandles or misuses personal data. Under such circumstances, the federal agency can even be held liable.[350] Both acts are extremely relevant to protect privacy rights against rapid, technological developments, which may tend to create a "surveillance environment" for the individual. However, one can question what would happen if a US INSPASS user who is not a resident nor a citizen of the United States requests access to the information contained by the US government, or claims infringement of privacy rights performed by the latter. Obviously these acts do not have extraterritorial application, hence, the foreign user of US INSPASS could not avail himself of the provisions contained therein.[351]

4.4.3. Private Sphere of US Privacy Laws

The private sphere of the protection of privacy is governed by the law of torts and some specific sectoral regulations, which will be carefully examined herein.[352] As expressed previously, the right of privacy started to develop after the publication of the seminal article of Warren and Brandeis; however, courts did not immediately embrace the principles contained therein. Thus, a New York court rejected the existence of the right of privacy in *Roberson* v. *Rochester Foling Box Co.*[353] It was only in a landmark case in the state of Georgia, *Pavesich* v. *New England Life Insurance Co.*,[354] that the judicial recognition of the right of privacy

---

[349] The Privacy Act establishes limitations on the disclosure of data by federal agencies. According to the act "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to any other agency, except pursuant to a written request by, or with the prior written consent of, the individual to who the record pertains." 5 U.S. § 552a (b). For case law reference, see *Ray* v. *Department of Justice*, 720 F.2d 216 (D.C. Cir. 1983); *American Federation of Government Employees* v. *U.S. Railroad Retirement Board*, 742 F. Supp. 450 (N.D. III. 1990).

[350] See *Fitzpatrick* v. *Internal Revenue Service*, 665 F.2d 327 (11th Cir. 1982); *Albright* v. *United States*, 732 F.2d 181 (D.C. Cir. 1984). In both cases the courts were faced with improperly disclosed information by Federal Agencies and held them liable.

[351] See 5 U.S.C. 552a(a)(2).

[352] The right of privacy among private individuals has evolved in the field of common law torts as a development of well-established concepts of trespass to the person or property, nuisance, breach of copyright, intentional infliction of emotional distress, and infringement of patents or trademarks. See R.F.V. Heuston & R.A. Buckley, *Salmond & Heuston on the Law of Torts*, 20th ed. (London: Sweet & Maxwell, 1992) at 36.

[353] See *Roberson* v. *Rochester Folding Box Co.*, 171 N.Y. 538 at 564 (Super. Ct. N.Y. City 1893).

[354] See *Pavesich* v. *New England Life Insurance Co.*, 122 Ga. 190, 50 S.E 68 (1905).

through the application of the law of torts was founded, becoming the leading case thereafter.[355]

4.4.3.1. The Law of Torts

In 1960 William Prosser attempted to classify the tort of privacy into four categories: 1) intrusion upon seclusion, solitude, or private affairs, which must be offensive and objectionable to a reasonable man; 2) public disclosure of private facts; 3) false light publicity; and 4) appropriation for the defendant's benefit of the plaintiff's name or likeness.[356] The first category is an evolution from the original tort of trespass, which has evolved from its original physical context and now includes eavesdropping of private conversations.[357] This is perhaps the most suitable sort to include infractions to the right of privacy by means of implementing automation devices since the categorisation includes intrusion into the individual's personal affairs, thereby enlarging its scope of applicability. Notwithstanding the forgoing, the offensive and objectionable requirement would seem to create a somewhat cumbersome burden for the plaintiff to overcome.[358] Hence, in *Cox Broadcasting Corp.* v. *Cohn*,[359] the US Supreme Court held that the plaintiff must demonstrate "unreasonable intrusion" into one's affairs and later disclosure of the material gain. On the other hand, the courts are given the "reasonableness" discretionary safety net. The second sort of Prossner's classification involves the revelation of private facts to public knowledge; even when those are true, they cannot be used as a defence.[360] In *Sidis* v. *F-R Publishing Corp*,[361] the court held the someone's privacy was not violated by a newspaper or magazine publishing a correct account of one's life or doings, except under "abnormal circumstances", which did not exist in this case.[362] Subsequently, the third of Prossner's categories tackles publicity when the defendant places the plaintiff in the "false light of the public eye", which

---

[355] Later, the Restatement of Torts recognised its existence. See *Restatement (First) of Torts* (1939).
[356] See W.L. Prosser, "Privacy" (1960) 48:3 Cal. L. Rev. 383 at 389.
[357] See W.L. Prosser, *The Law of Torts*, 4th ed. (St. Paul, Minnesota: West Publishing, 1971) at 807 [hereinafter *Law of Torts*].
[358] See generally J.R. Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" (1992) 44 Fed. Com. L. J. 195 at 224.
[359] See *Cox Broadcasting* v. *Cohn*, 420 U.S. 469 (1979).
[360] See *Law of Torts*, *supra* note 357 at 809.
[361] See *Sidis* v. *F-R Publishing Corp.*, 113 F.2d 808 (2nd Cir. 1940).
[362] It is interesting that the defence pled that the public had a right to know the story, an argument embraced by the court, confirming the newsworthiness of the information. See E. Karafiol, "The Right to Privacy and the SIDIS Case" (1978) 12 Ga. L. R. 513 at 520-526.

is indeed related to defamation, although not a prerequisite thereof.[363] The last of Prossner's class addresses the financial gain obtained from publicising the plaintiff's name or likeness. None of the last two categories seem to directly create a cause of action for breaches created by the application of automation devices.

Although a very scholarly classification and its later adoption in the Restatement Second of Torts,[364] as well as in numerous State statutes within the United States, the flaw in Prossner categorisation lies in the fact that it is extremely difficult to accommodate each case into one particular category, as has already been observed by some commentators.[365] But perhaps one of the most valuable contributions of the Prossner studies, particularly for the purposes pursued herein, has been the identification of possible defences and their implications when dealing with common law privacy tort cases. More specifically, Prossner has noted that consent given by the plaintiff, particularly within the context of a contractual relationship, would bar any claim of privacy infringement under the basis of publicity, appropriation, or intrusion; only when such invasion of privacy goes beyond the terms of the contract, as originally contemplated, would intrusion be recognised by the courts as not effective to avoid liability.[366] In the *Sidis* case, for instance, the court failed to analyse whether the plaintiff gave consent for the publication, thus inferring that "consent" is a defence for cases of invasion of privacy of mass publication.[367] Similarly, in *Ault* v. *Hustler Magazine*[368] the Court rejected a claim on the basis of intrusion because the plaintiff agreed to be photographed.

The preceding discussion is of paramount significance for the protection of privacy rights in the automation context of air transport, specifically because most of the endeavours undertaken therein involve complex contractual provisions *inter partes*. The airline smart card holder would normally express his or her written consent to the other party in order to

---

[363] See *Law of Torts*, *supra* note 357 at 812.
[364] See *Restatement (Second) of Torts* § 652 (1977). See also W. Prosser, "The Right to Privacy" (1960) 48 Cal. L. Rev. 383 at 390.
[365] For a criticism of William Prosser's classification, see E.J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U.L. Rev. 962.
[366] See *Law of Torts*, *supra* note 357 at 817. Although less relevant for the purposes pursued herein, another defence of the appropriation type constitutes newsworthiness. See R.L. Moore, *Mass Communication Law and Ethics* (Mahwah, New Jersey: Lawrence Erlbaum Associates. 1999) at 396.
[367] See Karafiol, *supra* note 362 at 529.
[368] See *Ault* v. *Hustler Magazine, Inc.* 860 F.2d 877 (9th Cir. 1988).

employ the services offered. However, contractual provisions containing the consent clause often have a "Lilliputian"[369] font type, making it almost unnoticeable to the consumer; this situation could hamper a future claim pursued by the latter.[370] Similarly, one can question to what extent the data subject expresses consent when being inspected at the airline check-in counter where his/her machine-readable passport is either scanned through a reader device or the data is manually input into the airline computer system, information that in the case of the API programme is ultimately sent by electronic means to the government authorities at the passenger's port of destination. In most circumstances the airline employee does not ask the passenger whether he or she would like to comply with the API programme, nor is an alternative choice given to the latter. The passenger is thus faced with no other option but to comply with the airline requirements in order to board his flight. It will be interesting to see whether the American courts will consider the foregoing discussion as direct or indirect consent in case a privacy tort claim arises, an issue that could have tremendous significance when examining tort claim cases. For instance, in *Fontan de Maldonado* v. *Lineas Aereas Costarricenses S.A.*,[371] the US court held that the provisions addressing the airline's tariffs filed with the US Department of Transportation constitute a binding contract between the air carrier and the passenger, even though the latter was unaware of the contents of such tariff provisions.[372] If one were to apply the *rationale* of the ruling held in *Fontan de Maldonado* to privacy cases, the courts in the United States would most likely tend to reject tort claims on the basis of the "consent defence theory", undoubtedly established in US jurisprudence. Therefore, private entrepreneurs and the public authorities involved will be extremely keen on being cautious when drafting the aforesaid clause in order to relieve themselves from liability of any privacy claim that may arise. Furthermore, some commentators have expressed concern about the effectiveness of the common law tort system to protect privacy rights of the individual, particularly in the information era.[373] This thesis contends that the tort remedy under infringement of a privacy right places an exceptionally onerous burden on

---

[369] The term "Lilliputian" appeared in the American case *Lisi* v. *Alitalia*, where Judge MacMahon characterised the small letter font of the conditions of contract as being "camouflaged in Lilliputian Print". *Lisi* v. *Alitalia*, 370 F. 2d 508 (3d Cir. 1966) at 13.

[370] *A contrario*, the defendants will advocate the sustainability of the freedom of contract principle, which is to be governed by the parties' relationship in case a tort claim arises.

[371] See *Fontan de Maldonado* v. *Lineas Aereas Costarricenses S.A.*, 936 F.2d. 630 (1st Cir. 1991)[hereinafter Fontan de Maldonado].

[372] See R.I.R. Abeyratne, "Recipient States' treatment of Inadmissible aliens and Refugees" (1999) 12:4 Int'l J. Politics, Culture & Society 613at 617.

[373] See C. Martin, *supra* note 272 at 820.

the damaged party, who must prove the offensiveness of the intrusion, and overcome the insurmountable legal hurdle of the "consent defence theory" in most circumstances. The US tort system places the damaged party under inferior circumstances that are somewhat difficult to defeat.[374]

The scenario gets even more complex in analysing the possibility of tort claims brought in the United States by foreign individuals on the basis of infringement of privacy rights. The latter situation is quite likely to happen in such an international environment as air transport where automation endeavours are taking place. The courts will then have to analyse the labyrinth of provisions addressing conflict of laws and jurisdictions on a case-to-case basis. However, there is a general understanding that a tort claim can be brought following the Roman principle of *"lex loci delicti comissi"* and at the domicile of the tortfeasor. Notwithstanding all the inconveniences and economic burdens of bringing a lawsuit in a foreign jurisdiction, the damaged party could certainly pursue a claim thereto, but one can certainly question the chance of success.

4.4.3.2. United States Private Sphere Statutes

Additionally, the United States has enacted patchwork sectoral privacy protection legislation seeking to cover certain areas of the somewhat infinite spectrum of interactions where private individuals could experience violation of privacy rights. Although not directly relevant to the implementation of automation devices in air transport, the *Fair Credit Reporting Act*[375] was enacted to regulate the handling of privacy data by credit reporting agencies. Subsequently, the *Right to Financial Privacy Act*[376] was passed in 1978, seeking to ensure that financial institutions notify their customers before any information is provided to government agencies. This act is relevant to the protection of privacy under the automation endeavours in air transport since it includes financial institutions such as banks, which may be the issuers or administrators of smart cards performing the functions of credit cards.

---

[374] Although this thesis argues the inadequacy of the US tort system to respond to privacy claims, some commentators have indicated the flexibility and adaptability of the latter to confront emerging challenges. See *contra* W.J. Fenrich, "Common Law Protection of Individual's Rights in Personal Information" (1996) 65 Fordham L. Rev. 951 at 1003.

[375] See 15 U.S.C. 1681 (1988).

Perhaps the most significant privacy protection sectoral legislation enacted in the United States constitutes the *Electronic Communications Privacy Act of 1986*[377] This hybrid act includes the activities conceded by private parties as well as their relationship with the federal government covering all forms of electronic communication,[378] such as e-mail, digitised images, and EDI.[379] It forbids the unauthorised interception, use, storage, and disclosure of electronic communication while in transit or in storage.[380] The act goes further to grant civil action recovery to persons or entities whose "electronic communication have been intercepted, disclosed, or intentionally used".[381] Section 2701 of the act provides criminal penalties for infringement thereof.

Since this act includes the transmission of EDI, the endeavours undertaken by ICAO to promote its use through Annex 9 of the Chicago Convention and the API System in the United States would *a priori* seem to be included within the act's scope. However, the scenario is extremely complex, and thus the applicability of the act is rather uncertain. All the aforesaid initiatives envision the electronic transmission of data by international air carriers to national government agencies, or foreign government agencies, the latter being the case when the air carrier is from a different country. If the data transmitted to and from the United States by electronic means does not refer to a citizen of the United States or resident thereof, the act is inapplicable. Moreover, the courts have consistently ruled that the *Electronic Communication Privacy Act* does not have any extraterritorial application.[382]

---

[376] See 12 U.S.C. 3401-3422.

[377] See 18 U.S.C. 2510-2521. The Electronic Communications Privacy Act constitutes an enlargement of the scope of protection of the Wiretap Act of 1968. See R.S. Sterre, *infra* note 379 at 249.

[378] Electronic communications is defined as:

> any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in par by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include a) any wire or coral communication; b) any communication made through a tone-only paging device; c) any communication from a tracking device; or d) electronic funds transfer information stored by a financial institution in a communications system used for electronic storage and transfer of funds.

18 U.S.C. 2510(1).

[379] See R.S. Sterre, "Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act" (1998) 33 Val. U. L. Rev. 231.

[380] See J. Rosenoer, *Cyber Law* (New York: Springer, 1997) at 133.

[381] 18 U.S.C. 2520 (a). The act even permits the recovery of punitive damages. See *Jacobson* v. *Rose* 592 F.2d 515 (CA9 Nev., 1978).

[382] See *United States* v. *Cotroni*, 527 F.2d 708 (CA2 NY., 1975); *United States* v. *Toscanino*, 500 F.2d 267, (CA2 NY, 1974); *Stowe* v. *Devoy*, 588 F.2d 336 (CA2 NY, 1978); *United States* v. *Delaplane*, 479 U.S. 827 (1986); *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144, (DC Dist. Col, 1976); *United States* v.

Bearing in mind that those initiatives involved a conglomerate of participants, where the data subjects were from numerous countries, the protection and safeguards offered by the sectoral patch legislation of the United States does not offer adequate protection of privacy rights to US citizens, nor to foreign individuals, against the emerging trends of automation in facilitation of air transport. [383]

4.4.4. United States Privacy Law Critical Assessment

The foregoing discussion supports the argument that privacy protection in the United States with its two-fold approach between the public and private sphere is exceedingly dense and convoluted. However, this thesis favours the idea that the US legal framework within the public sphere, addressing the protection and access to informational privacy data held by government agencies protects the individual's right and ensures the granting of remedies for cases of infringement, as long as he or she is a citizen or resident of the United States. It is worth mentioning that the endeavours undertaken in implementing automation in facilitation of air transport comprise a multiplicity of players from different countries, not solely from the parochial United States. Since those acts were enacted to protect and guarantee the rights of Americans, foreigners who happen to be affected by the endeavours in air transport would not have the same safeguards as their American counterparts.[384] Nevertheless, within the private sphere, uncertainty surrounds individuals confronted with privacy claims. The burdens of the plaintiff in a privacy tort case are extremely difficult to overcome. The sectoral patchwork legislation enacted has flaws in numerous areas. Hence, this thesis sustains that the advancement of technology as envisaged in the air transport industry considerably compromises privacy right implications in the US legal context.

Bennet, 410 F. Supp. 144 (DC Puerto Rico, 1982); *United States* v. *Burford,* 755 F. Supp. 607 (SD NY, 1991); *United States* v. *Phillips*, 479 F. Supp. 423 (MD Fla., 1979).

[383] Other sectoral privacy legislation includes the *Cable Communication Policy Act of 1984*, the *Employee Polygraph Protection Act of 1988,* the *Telemarketing Protections Act of 1991,* and the *Video Privacy Protection Act of 1988*, but none of them are applicable to the automation initiatives herein examined.

[384] Some commentators have expressly indicated that the Privacy Act is not extended to protect foreigners. See R.M. Gellman, "Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules" (1996) 41 Vill. L. Rev. 129 at 164.

4.5. The European Privacy Approach

The privacy rights environment in Europe has taken a totally different direction to that of the United States. Europe, faithful to the long-standing civil law background of most of its countries, has always been keen on predicting the probable consequences of the emergence of particular novel phenomena, as has been reflected in the enactment of omnibus regulation, rather than letting law evolve as a consequence of judicial experiences. Europeans are fond of overprotecting, since to them the US model of self-regulation is tantamount to no regulation.

The European approach to privacy protection is deeply rooted in the reference made to the right of privacy in the *European Convention for the Protection of Human Rights and Fundamental Freedoms*,[385] whereby Article 8 establishes it as a fundamental human right.[386] Hence, Europeans tend to approach privacy as a primordial concern of mankind where as much foreseeable protection as possible is highly desirable.[387] With the introduction of the Convention, numerous countries in Europe started enacting regulation addressing privacy. [388]

---

[385] See *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S.5, art. 8.

[386] See also D. Feldman, "Privacy-related Rights and their Social Value", in P. Birks, ed., *Privacy and Loyalty* (Oxford: Clarndon Press, 1997) at 28.

[387] The European authorities have long expressed concern about the possible implications in the individual's privacy caused by the advancement of technology. Hence, The Committee of Experts on Human Rights reported in 1970 that the existing legal framework was inadequate to protect privacy rights. See Lloyd, *supra* note 301 at 45.

[388] The German State of Hese passed the first legislation in Europe addressing privacy data protection in 1970. Later, Sweden passed the Data Act of 1973; Germany enacted the Federal Data Protection Act in 1977; France passed the Law on Informatics, Data Banks and Freedoms, and Austria endorsed the Data Protection Act both in 1978; finally Great Britain established the Data Protection Act of 1984. See V. Mayer-Schonberger, "Trans-Atlantic Information Privacy Legislation and Rational Choice Theory" (1999) 67 George Wash. L. Rev. 1309 at 1316. See generally J.A.L. Sterling, *The Data Protection Act 1984*, 2d ed. (Bicester, Oxfordshire: CCD Editions Limited, 1984); J. Freese, "Seven Years of Swedish Data Legislation – Analysis of Impact and Trend for the Future" in *Informatique et Protection de la Personnalité* (Saint-Paul Fribourg: Editions Universitaires Fribourg Suisse, 1981) at 69; J. Velu, *Le Droit Au Respect De La Vie Privée* (Brussels, Belgium: Presses Universitaires de Namur, 1974) at 19; R. Wacks, *Personal Information* (Oxford: Clarndon Press, 1989) at 39; D.H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill, North Carolina: The University of North Carolina Press, 1989); F. Rigaux et al., *La Vie Privée, une liberté parmi les autres?* (Brussels: Maison Larcier, 1992); P. Seipel, ed., *From Data Protection to Knowledge Machines* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990); Y. Poullet, "Data Protection between Property and Liberties" in H.W.K. Kaspersen & A. Oskamp, eds., *Amongst Friends in Computers and Law – A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990) at 161.

Later, the Council of Europe, pursuant to Resolution 73/22, adopted the *Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data*,[389] based on OECD model recommendation guidelines, on 28 January 1981.[390] Although the Convention included only automated processing of data, leaving the manual one out of its scope; it set forth the early goals pursued by the European Authorities, identifying many of the issues that remain relevant in modern legislation nowadays. However, the main flaw of this instrument lies in the fact that it was only ratified by a small number of countries, and hence, failed to achieve a standard degree of privacy protection within Europe.[391] Therefore, the European Commission acknowledged the necessity to take further actions to achieve such goals by requiring States to harmonise privacy data legislation. Thus, the path was set for the advent of the European Privacy Data Directive. [392]

4.5.1. The European Privacy Data Protection Directive

On 24 October 1995 the European Parliament and the Council passed Directive 95/46 on the protection of the processing and movement of personal data.[393] The intention of the EC Directive's framers was to equalise the disparity of levels of privacy data protection within Europe, whereby countries such as France and Germany had very comprehensive legislation, but others like Italy and Greece had none. The EC Directive,

---

[389] See Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Europ. T.S. No. 108 (28 January 1981) [hereinafter *European Convention*]. Later, the EC Commission recommended that States adopt the aforesaid Convention, understanding that the establishment of the common market calls for an extensive standardisation of the conditions obtaining in relation to data processing at the European level. The *rationale* of the European efforts lies in the fact that the data protection is desirable so that there can be free movement of data and information across frontiers and in order to prevent unequal conditions of competition and the consequent distortion of the common market. See EC, *Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*, [1981] O.J. L. 246/31.

[390] See also EC, *Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 1981); EC, *New technologies: a challenge to privacy protection?* (Strasbourg 1989). See generally EC, *Protection of personal data used for social security purposes* (Strasbourg, 1986)

[391] See P.P. Swire & R.E. Litan, *None of Your Business* (Washington, DC: Brookings Institution Press, 1998) at 24.

[392] The term "Data Protection" has been highly criticised among scholars for giving the connotation that what is really protected is the information rather than its subjects. See Lloyd, *supra* note 301at 38.

[393] See EC, *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31 [hereinafter *EC Directive*].

which came into force in 1998, gives substance to and amplifies those provisions contained in the European Convention. The enactment of the directive was chosen by the European Commission in order to permit States to level their legislation with the minimum standards set within the Directive's legal framework thereof.[394] The aim of the EC Directive is to harmonise the existing law of its Member States.[395] It is the responsibility of each Member State to develop its own privacy data legislation in accordance with the Directive, which lays out the legal model to follow. However, one can reasonably foresee the emergence of numerous disparities when each county enacts its own legislation, a situation that could be aggravated when different administrative agencies and courts are called on to interpret the provisions contained therein.

4.5.1.1. Objective

The EC Directive seeks to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".[396] As clearly identified by Schwartz and Reidemberg, the Directive has four main purposes: 1) to create norms for collecting and processing personal data;[397] 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.[398] This thesis will proceed to comprehensively analyse the provisions relevant to the emerging trends on automation in facilitation of air transport.

---

[394] The competency of the Directive, found in Article 7(a), lies in the European Union, which aims at promoting the free movement of goods, persons, services, and capital; therefore, it is envisaged that personal data should flow freely from one member State to another, but it also acknowledges the necessity to safeguard the rights of individuals in accordance with the *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S.5, art. 8. See *Treaty Establishing the European Union*, 2 October 1997, art. 14.

[395] See Simitis, *supra* note 292 at 448.

[396] It is worth mentioning that the protection of privacy rights of legal persons falls outside the scope of the Directive. See *EC Directive*, *supra* note 393, art. 1.

[397] According to the definitions contained in the Directive, the term personal data refers to "any information relating to an identified or identifiable natural person", clarifying that an identifiable person is "someone who can be identified, directly or by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity". See *EC Directive*, *supra* note 393, art. 2(a).

[398] See P. Samuelson, *supra* note 309 at 763.

4.5.1.2. Scope of Application

The scope of applicability of the EC Directive is extended to personal data wholly or partly processed[399] by automatic and manual means, as long as they form part or are intended to form part of a filing system.[400] This constitutes a major difference from its predecessor, the European Convention, which was solely intended to cover the automatic processing of personal data. The enlargement of the scope of applicability is justified on the basis that drawing the line between manual and automatic processing is sometimes rather complex. Furthermore, the EC Directive presents a two-fold exclusionary approach: 1) it is not applicable to activities that fall outside of the scope of Community law, and matters concerning the State, such as public and national security, defence, economic well-being of the state involved, criminal investigation and breaches of ethics in the regulated professions; and 2) it is not applicable to any data related to purely personal or household activities.[401] The exclusion of the Directive's scope of issues, such as defence, national security and criminal investigation *per se*, removes ambiguity for future judicial interpretations, which may clarify the application of national privacy data protection laws in a large number of cases. *A contrario*, American courts are often faced with the necessity to formulate juridical tests, in order to confront and balance those interests.

4.5.1.3. Jurisdiction

The EC Directive undoubtedly establishes its jurisdiction by denoting that the law of each Member State shall be applicable as long as: 1) the processing is carried out by a

---

[399] The term processing of personal data is referred as: "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". *EC Directive*, *supra* note 393, art. 2(b).

[400] A filing system means "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis". *Ibid.*, art. 2(c).

[401] See *ibid.*, art. 3. Some commentators have already expressed profound concern about the fact that sometimes it can be extremely difficult to distinguish between purely personal or household activity and the normal endeavours individuals undertake through the normal course of their labour activities. For instance, the use of a laptop could best illustrate the complexity of the scenario. See Swire & Litan, *supra* note 391 at 70.

controller[402] in the territory of a Member State; or 2) the controller is not located in a Member State's territory, but in order to process data uses equipment that is located in the territory of a Member State. In addition, the controller has to nominate a representative for cases where he does not operate directly in the territory of a Member State, but rather uses equipment located therein.[403] *Ab initio*, the EC Directive's jurisdiction specifications pose significance consequences for the air transport sector, particularly considering its feasible extraterritorial applications. For example, and bearing in mind the enormous amount of personal passenger information that carriers handle,[404] an international airline such as Aerolineas Argentinas may use an Amadeus Computer Reservation System (CRS), owned and controlled by European carrier such as Lufthansa. Hence, even though Aerolineas Argentinas, the controller, is located outside the territorial jurisdiction of the European Union, the provisions contained in the EC Directive will be directly applicable, because unarguably the non-European carrier is using automated equipment situated in the territory of a Member State for the purpose of processing personal data.[405] One can certainly foresee that the European authorities will most likely favour the extension of such extraterritorial application to the non-European carrier, when the latter handles the personal data of Member States' citizens. Furthermore, the EC Directive will even be applicable to cases where a non-European airline has a frequent flyer smart card sponsored by a European bank. The possibilities and combinations are endless, but the foregoing examples remain common practices in the air transport industry.

4.5.1.4. Quality of Data Processed

In addition, the EC Directive sets forth principles related to the quality of data, emphasising that it can only be collected for the specified, legitimate, explicit purposes, and that such accurate, up-to-date collection must be adequate and not excessive in relation to

---

[402] The term controller is referred as: "a natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data". See *EC Directive*, *supra* note 393, art. 2 (d). From the language of the provision, it is clear that the EC Directive is applicable to both private organisations and government agencies that process personal data of individuals.

[403] See *ibid.*, art. 4.

[404] See Swire & Litan, *supra* note 391 at 132.

[405] As a matter of fact, negotiations are underway between Amadeus corporate executives and the European authorities in order to reach an agreement viable for both parties. See Swire & Litan, *supra* note 391 at 133.

the purposes thereof. The responsibility to comply with the aforesaid standards rests with the controller, who may be solely or jointly liable in case of infringements.[406]

4.5.1.5. Unambiguous Consent Principle

Perhaps one of the most remarkable requirements of the EC Directive is the fact that data can only be processed when the data subject has "unambiguously given his consent".[407] Nevertheless, several exceptions to this rule are provided, permitting the data to be transferred without the data subject's consent as long as: 1) processing is necessary for the performance of a contract where the data subject is a party thereto; 2) processing is necessary to fulfil the controller's legal obligation; 3) processing is necessary to protect the vital interest of the data subject; 4) processing is necessary for the public interest; and 5) processing is necessary for a legitimate interest of the party to whom the data will be disclosed, provided it does not outweigh the interest of the data subject.[408] The EC Directive intends to eliminate as much vagueness from the formulation of the consent as possible, whereas in the United States the interpretation of the consent rule is solely scrutinised by the judiciary. However, it remains to be seen how the EU administrative agencies and the courts will interpret the "unambiguous consent" rule. For instance, according to IATA's General Conditions of Carriage,[409] established as a recommended practice among its member in order to determine the contractual provisions between the parties, the passenger "authorises the air carrier to retain and transmit his personal data to its own offices, other carriers or the providers of such services, in whatever country they may be located".[410] One may question how the administrative authorities and the courts will interpret this "camouflaged consent", enclosed in an adhesion contract where the passenger has no other choice but to agree with the provisions thereof.[411] Hence, the strict recognition of such consent will be tantamount to the incontestable capability of the air carrier to freely transfer the passenger's personal data,

---

[406] See *EC Directive*, *supra* note 393, art. 6.

[407] The EC Directive defines the data subject's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". *Ibid.*, art. 2(h).

[408] See *ibid.*, art. 6

[409] See IATA, *General Conditions Of Carriage*, Recommended Practice 1724.

[410] See *ibid.*, art. 6.3

[411] See P.P.C. Haanappel, "The IATA Conditions of Contract and Carriage for Passengers and Baggage" (1974) 9 Eur. Transp. L. 650 at 652. See also P. Aronstam, *Consumer Protection, Freedom of Contract and*

common practice in the air transport industry. For the case described herein, this thesis sustains the inapplicability of constructing the adhesion contractual provisions to represent "unambiguous consent" because it places the data subject in an inferior situation without any opportunity to challenge the collection of data. Should the definition of informational privacy be adopted for these situations, the data subject must be given the opportunity to control information about himself. Still, one must recognise that when facing legal action, the defendants will favour the adoption of the freedom of contract principle.[412] This thesis also acknowledges that not extending the adhesion contractual provisions to represent "unambiguous consent" will cause severe modification in air carriers' common procedures, which might have serious financial implications.

In cases where the passenger is required to present his passport at the airline check-in counter, to be scanned through a reader device, or the data is manually input in order to comply with the API programme, one may rightly question to what extent that constitutes a processing necessary for the performance of a contract to which the data subject is party thereto. Certainly, the passenger is obliged to present his personal documentation to prove his real identity before boarding a particular flight as provided by the conditions of contract;[413] however, one can question whether the airline has the right to record the passenger's personal data and *a fortiori* send the information overseas without obtaining the "unambiguous consent". This thesis supports the idea of a limited interpretation of the extension of the contract, hence, the "recording of data" does not constitute *per se* part of the contract to which the passenger is a party; nor can the airline avail itself of the exception contained under the EC Directive, by claiming that the "processing is necessary for the compliance with a legal obligation to which the controller is subject to", because the airline is merely an intermediary, thus, a processor,[414] not an operator. The latter will most likely be a US authority for purposes of the API system.

---

the Law (Cape Town: Juta & Company, 1979) 16; S.D. Liyanage, *International Airline Code-Sharing* (LL.M. Thesis, McGill University 1996) [unpublished].

[412] It will also be interesting to see to what extent international air carriers have adopted the IATA Recommended Practice 1724, thereby including the aforesaid adhesive contractual provisions.

[413] See IATA, *supra* note 409, art. 14.2

[414] An operator under the provisions established by the EC Directive refers to: "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller". *EU Directive*, supra note 393, art. 2(e).

Similarly, an interesting case arose in Sweden where the Data Protectorate prohibited the transfer of computer reservation information to American Airlines Sabre headquarters in the United States because the air carrier did not obtain the passenger's consent in order to process the personal data, which included, *inter alia*, the passenger's name, itinerary, address, and method of payment, as required by Section 11 of the Swedish Data Act.[415]

On the other hand, the scenario is somewhat simpler when analysing the privacy legal implications of implementing smart cards even as envisioned with the biometric measurement devices, essentially due to the fact that extremely thorough contractual provisions will most likely govern the relationship between the card holder, the issuer, the airline involved and perhaps even the government authority. This thesis has already carefully explained the endeavours having taken place in the Netherlands and in Finland to implement the electronic European identification travel card, where both governments are acutely conscientious of obtaining the "unambiguous consent" of the user. Therefore, one can effortlessly envision that the European authorities will pressure the airlines and players in the air transport sector to properly notify the data subject of all the processing taking place with respect thereto, by means of stringent "notices", whereby the data subject is granted the opportunity to express his unambiguous consent, or otherwise reject the service offered on the basis that it may violate his privacy rights.[416]

4.5.1.6. Processing of Sensitive Data

Although certain exemptions are provided, the EC Directive also establishes certain special type of personal data for which processing is prohibited, *inter alia*, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the

---

[415] See Decision of the Administrative Court of Appeals, Stockholm, Case No. 2104-1996 (23 April 1997) cited in P.P Swire & R.E. Litan, *supra* note 391 at 133. See also Cate, *supra* note 300 at 193.

[416] If that were the case, it would be interesting to see requirements placed on air carriers by the European authorities in order to adequately notify the passenger of the collection of personal information. Whether a verbal notification when the passenger is booking a reservation, or a written notice included in the passenger ticket or itinerary receipt would suffice remains to be tested. The foregoing would undoubtedly create a tremendous modification on the air carriers common practices and procedures, which could have significant economic costs.

processing of data concerning health or sex life.[417] It goes further to encourage Member States to reconcile the conflictive interest between the individual's right of privacy and societal freedom of expression.

4.5.1.7. Data Subject's Bill of Rights

The EC Directive grants a large number of privacy rights to the individual, and thus could be labelled as the "Data Subject Bill of Right". Hence, the individual is bestowed the right to know the identity of the controller and his representative, and the purposes of processing for which the data is required.[418] In other words, when air carriers' employees swipe the passport through the reader device or input the data manually to comply with API procedures, they ought to inform the data subjects of the purpose for which such data is collected, which in practice does not usually happen. Similarly, in more complex situations, such as smart cards with biometrics embedded therein, the controller should notify the data subject of who is handling the information and for what purposes, which could be somewhat difficult to determine due to the large number of players involved. For instance, as envisaged in the SPT initiative, a myriad of balkanised players will be handling passenger data on a "need to know" basis, which can raise tremendous difficulties when establishing who the controller is. Furthermore, Abeyratne has noted that the MRTD-issuing State is legally obliged to inform the bearer of the details enclosed therein.[419]

Similarly as provided by the FOIA in the United States, the EC Directive grants the individual the right to access information handled by the controller. The main difference between the previously mentioned two legal regimes lies in the fact that the former only includes activities undertaken by the government and its agencies, whereas the latter is particularly directed at private and public organisations that happen to store, control, or process the individual's personal data.[420] The data subject bill of rights permits the request

---

[417] See *EU Directive*, *supra* note 393, art. 8(1). Needless to say that air carriers handle such sensitive passenger personal information, *e.g.*, religious and medical data.
[418] See *ibid.*, art. 10.
[419] See Abeyratne, *supra* note 117 at 22.
[420] See *EU Directive*, *supra* note 393, art. 12(a). Similarly, numerous other countries, such as Argentina, Brazil, Paraguay, and Colombia concede the right to access the information the government and its agencies have on the data subject through the legal institution of the *"Habeas Data"* as a cause of action, which translated from Latin means "bring me the data". In some countries the *Habeas Data* has been extended to include processing of personal data by private parties, although the latter constitutes a constant doctrinal

for correction, and erasure of any data processing, that is not in accordance with the provisions enclosed in the EC Directive.[421] Additionally, the data subject may object to the processing of personal information at any time as long as he has legitimate grounds to do so.[422] It is important to remark that the data subject bill of rights legally empowers the individual against possible invasions, intrusions, or infringements of privacy rights, whereas the burden is placed on controllers and processors of data, a situation that is totally different in the United States. [423] Therefore, one can easily expect that privacy claims will more likely succeed within the legal spectrum given by the EC Directive. In addition, the person acting under the authority of the controller or the processor must assure the confidentiality of processing, responding only to the instructions and orders of the controller, making the latter responsible in the event of any infringement of privacy rights.[424] The foregoing *ab initio* has direct implications for the air transport automation surroundings since almost all of the facilitation initiatives envision the inclusion of a large number of persons dealing with massive amount of personal data.

Security concerns are also addressed by obliging controllers to provide appropriate technical and organisational measures to avoid potential information leaks, thereby protecting personal data, which is particularly crucial for the convoluted air transport environment.[425] One of the most notorious achievements of the EC Directive has been the establishment of Supervisory Authorities, which are the bodies responsible for monitoring the compliance with the provisions enclosed therein.[426]

---

debate among scholars. It was first established in the Portuguese Constitution of 1976, then taken by the Spanish of 1978, and subsequently to a large number of countries particularly in South America. See J.A. Moreno Rufinelli, *Nuevas Instituciones de la Constitución Nacional* (Asuncion, Paraguay: Intercontinental Editora, 1996) at 145. See also *Constitutional Act, 1994* (Argentina), art. 43; *Constitutional Act, 1976* (Portugal), art. 35; *Constitutional Act, 1978* (Spain), art. 18(4); *Constitutional Act, 1991* (Colombia), art. 25; *Constitutional Act, 1992* (Paraguay), art. 135.

[421] See *EU Directive*, *supra* note 393, art. 12(b).

[422] See *ibid.*, art. 14.

[423] See M.P. Roch, "Filling the Void of Data Protection in the United States: Following the European Example" (1996) 12 Computer & High Tech. L.J. 71 at 83.

[424] See *EC Directive*, *supra* note 393, art. 16.

[425] See *ibid.*, art. 17.

[426] See *ibid.*, art. 28(1). For instance, the controller or his representative must inform the Supervisory Authority before carrying out wholly or partly any automatic processing of personal data, which applied to the air transport sector means that each incumbent in the business must first identity who is the controller of the personal data, to later notify the supervisory authority in its respective country. See *ibid.*, art. 18. The contents of the notification should include the name and address of the controller and of his representative, the purpose of the processing, a description of the categories of the data relating to the data subject, the recipient of the categories, and any proposed transfers of data to third countries. See *ibid.*, art. 19.

4.5.1.8. Legal Remedies

The EC Directive specifically mandates each Member State to confer the necessary legal remedies against any breaches of privacy rights.[427] The data subject is entitled to receive compensation from the controller in case damage is sustained. Although the burden of proof is on the controller's side, he may be exempt if he proves that he is not responsible for the damage.[428] This is the pro-data subject spirit of the EC Directive, which grants not only fundamental rights for the protection of privacy, but also provides the mechanisms to correct any deviation of the system. Perhaps this is one of the advantages of creating a specific legal framework to deal with an emerging problem or, where every situation has been carefully studied, of trying to envision all the possible derivatives; *contrario sensu*, in the United States the approach has been to let the existing legal system respond to each rising difficulty and develop from experience. However, the detractors of the former would argue that this type of legal framework is rather static and non-flexible, handicaps that do not allow the judiciary to adapt themselves quickly enough to emerging technological advancements. The latter will always precede the enactment of legal rules and the entrepreneurial air transport sector will not favour a stationary business attitude awaiting legal regulations to solve the raising problems.

The EC Directive asserts that Member States, through the application of their national laws, must guarantee the Directive's full implementation, and must also impose sanctions in case of infringements.[429] This obligation placed on Member States represents a risk for controllers, who will be forced to demand that insurers extend insurance coverage against any possible liability that might arise thereof, thus swelling premium rates and thereby affecting operational cots.[430] The preceding discussion could worsen the economic well-being of the air transport industry.[431]

---

[427] See *ibid.*, art. 22.
[428] See *ibid.*, art. 23.
[429] See *ibid.*, art. 24.
[430] See EC, *Handbook on cost-effective compliance with Directive 95/46/EC*, (Annex to the Annual report 1998 of the working party established by Article 29 of Directive 95/46/EC) at 58 [hereinafter *EC Handbook*].
[431] For a detailed study on the economic of the airline industry see R. Doganis, *Flying Off Course*, (London: Routledge, 1991).

4.5.1.9. Transborder Data Flows

Unarguably the most conflictive provision of the EC Directive addresses the issue of transborder data flows. The latter has been conceptualised as the transfer of data across national borders,[432] since transborder data flows directly trigger numerous endeavours related to automation in facilitation of air transport. This thesis will proceed to examine the implications thereof.

Although several exceptions are provided therein, the EC Directive embraces the principle that the transfer of data can only take place when a third country "ensures an adequate level of protection".[433] However, the language of the legal instrument fails to clearly define the concept of "adequate", leaving its interpretation to the supervisory authorities at the administrative level, and later to the judiciary when legal action is taken.[434] The Directive mentions that when assessing the degree of privacy data protection adequacy of third countries, Member States must take into account the nature of the data, the countries of origin and final destination, and the general and sectoral rules of law.[435] This *de facto* discretionary *potestas* bestowed upon Member States by the language of the EC Directive could easily provoke trade war between countries, whereby Member Sates would read the meaning of "adequacy" according to their economic interest. As a result, a large number of commentators have expressed serious concerns about the extraterritorial applications of the EC Directive and its direct implications for restricting the flow of information, thereby

---

[432] See J.L. Kraus, "On the Regulation of Personal Data Flows in Europe and the United States" (1993) Colum. Bus. L. Rev. 59, citing Justice M. Kriaby, "Legal Aspects of Transborder Data Flows" (1991) 11 Computer L.J. 233 at 235.

[433] See *EU Directive*, *supra* note 393, art. 25(1).

[434] The EC Directive bestows the Supervisory Authority with investigative powers, as well as decision-making with respect to, *inter alia*, imposing a temporary suspension on the processing of personal data provided it infringes the spirit of the EU Directive, reflected in the national legislation. See *ibid.*, art. 28.

[435] See *ibid.*, art. 25(2). Assessing the adequacy standard established by the Directive could be an extremely intricate task, particularly in countries where a sectoral regulation approach will not facilitate such appraisal. Certain industries may have a stringent level of regulation, whereas others are solely market controlled. See Martin, *supra* note 272 at 846; Reidenberg, *supra* note 290 at 498. Another criticism to the interpretation of the adequacy principle lies in the fact that controllers must identity third countries that are not in accordance therewith, either by making the decision themselves, or by consulting the Supervisory Authority guidelines. One can certainly foresee the tremendous uncertainties that controllers will face when dealing with these convoluted issues. Ultimately they will need to ask the Supervisory Authority for permission prior to making any transfer of personal data to countries whose regulatory framework is rather

hampering commerce.[436] Since the United States does not have a comprehensive privacy data protection legislation, one can argue that its standards are absolutely inadequate; such a strict interpretation would be a serious obstacle to the normal flow of information between the two world's largest markets. Moreover, if one were to construct the ideal data protection legal framework having Europe as a model, all the others would fall short to comply with the adequacy principle, since the European approach constitutes the most comprehensive and stringent one. The foregoing would represent considerable risks for the free flow of information, which is vital for numerous industries, particularly in air transport where automation initiatives strongly rely on the exchange of personal information among balkanised players. The EC Directive also demands that Member States and the Commission must exchange information about third countries that do not properly guarantee an adequate level of data protection,[437] which could lead to a *de facto* formation of black-listed nations. It is questionable how adequately the European authorities will consider some automation endeavours, such as the US INSPASS or the API system, where personal data of Member States' nationals might be severely exposed, according to the language of the EC Directive.

Nonetheless, the EC Directive affords the transfer of personal data to third countries possessing adequate standards when: 1) the data subject expresses his unambiguous consent; 2) the transfer is necessary for the completion of a contract between the data subject and the controller; 3) the transfer is necessary for the conclusion of a contract in the interest of the data subject; 4) the transfer is necessary to protect vital interests of the data subject; and 5) the controller pleads that adequate privacy protection safeguards have been clearly established in contractual provisions.[438] It has already been mentioned some of

---

uncertain; otherwise controllers could seriously be held liable of violating provisions contained in the EC Directive. See *EC Handbook*, *supra* note 430 at 59.

[436] See D.B. Rosler, "The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information" (1995) 10 High Tech. L.J. 105; P. Rose, "A Market Response to the European Union Directive on Privacy" (1999) 4 UCLA J. Int'l L. & For. Aff. 445; J.M. Fromholz, "The European Union Data Privacy Directive" (2000) 15 Berkeley Tech. L. J. 461; G.B. Trubow, "The European Harmonisation of Data Protection Laws Threatens US Participation in Trans Border Data Flow" (1992) J. Int'l. Bus. 159; M.J. Feeley, "EU Internet Regulation Policy: The Rise of Self-Regulation" (1999) 22 B.C. Int'l & Comp. L. Rev. 159; J.A. Zimmerman, "Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism" (1982) 4 J. Intl. L. Bus. 601; G. Pearce & N. Platten, "Achieving Personal Protection in the European Union" (1998) 36 J. Common Mkt. Stud. 529.

[437] See *EU Directive*, *supra* note 393, art. 25.3.

[438] *ibid.*, art. 26.

repercussions of the EC Directive in implementing automation in air transport with respect to the unambiguous consent principle, which is absolutely applicable when dealing with the foregoing exceptions on the transfer of data to third countries. Drawing the line between what constitutes part of a contract and what is necessary thereof may be remarkably difficult, since adopting stringent approach will considerably limit the transfer of data in multifaceted scenarios such as that of air transport, hence limiting the scope of the industry's operability. However, adopting an extreme liberal approach will make the EC Directive pure juridical literature without any enforceable degree of privacy data protection. One can foresee that the latter discussion will be part of exhaustive negotiations between the parties involved, where a *quid pro quo* compromise will most likely be made. Conceivably, one intriguing safety net enclosed in the exceptions to the transfer of personal data to third countries with inadequate standards represents the feasibility of establishing meticulous contractual provisions whereby the controller assumes the risk of guaranteeing the privacy rights of individuals, hence, availing liability and responsibility to himself. The latter constitutes a practicable way to circumvent the adequacy criterion, predominantly in countries where the technological infrastructure and legal framework is not yet available, but the resources of private enterprises permit taking on such a cumbersome risk. The contractual relationship must be entered into between the private enterprise and the European regulatory agency with competence in privacy data protection.[439] As a result, one can expect that international air carriers will most likely start lobbying the European authorities in an effort to conceive the drafting of thorough, detailed contractual clauses in order to permit the former to proceed with endeavours related to the implementation of automation in facilitation of air transport. Notwithstanding the benefits that "contractual" circumvention may offer to the flaws of privacy data protection, one can question the effectiveness of the remedies the data subjects could have, taking into account that they are not parties to the contractual relationship. *A priori*, the foregoing could constitute inaccessible legal barriers for data subjects to overcome; however, a further analysis reveals the contrary. Within the EC Directive legal framework, the European data subject could claim privacy infringement rights to the supervisory authority or another designated administrative body, which in numerous cases adopts the form of a "privacy commissioner" or a "privacy ombudsperson". The latter would be in

[439] In the aforesaid respect, Citicorp had reached a notorious agreement with the German data protection authorities; some commentators consider that it may serve as a future model agreement. See Swire & Litan, *supra* note 391 at 37.

charge of investigating, mediating, and eventually prosecuting private parties that could be violating the individual's right of privacy. Therefore, the fact that the data subject does not have a contractual relationship with the private organisation does not preclude him from pursuing privacy claims.

4.5.1.10. EC Directive's Flaws

One of the major flaws that the EC Directive has with respect to implementing automation initiatives in air transport, which is also faced within the US structure of privacy protection, lies in the fact that the European legal framework was obviously constructed to protect the interest of the Member States' citizens. The problem then arises, for instance, when a non-European individual claims infringement of his privacy rights by a European air carrier part of the SPT programme that happens to be the data processing controller. The latter falls under the EC Directive's scope of application, nevertheless, it is very unlikely that the EU administrative or supervisory privacy authorities will pursue claims against an EU private company, defending the privacy interest of non-European data subjects. The EC Directive also fails to balance the interest of data subjects and those of data users, since it creates barriers to transborder of personal data to third countries, by the application of a rather strict adequacy principle.[440] Although in its preamble there would seem to be an apparent inclination to balance both conflictive interest, in practice the EC Directive formulates the rule that personal data cannot be transfer to "inadequate countries".[441] The latter will create enormous difficulties for private organisations that may be in a position to properly protect the data subject's personal data, but whose country's legal framework is not in accordance with the provisions thereof. This thesis supports the argument the EC Directive is extremely prone to favour data subjects, inexorably leaving behind the interest of industry players.

Another interesting issue for the automation endeavours will be to observe whether the US Immigration and Naturalisation Service, in charge of developing the INSPASS

[440] It is worth mentioning that several reports carried out under the supervision of the Commission have expressed that one of the goals of the EC Directive was to achieve such balance. See EC, *The feasibility of a seamless system of data protection rules for the European Union,* (Study Contract ETD/95/B5-3000/MI/169) by Douwe Korff (Contractor, 1998) at 2.
[441] See *EC Directive, supra* note 393, Preamble 56.

programme, will pay attention to the specific data processing requirements in the EC Directive, particularly since a considerable part of the INSPASS market is formed by EU nationals.

4.5.11. EC Directive's Code of Conduct

In one of the most overlooked provisions, the EC Directive conceives the idea of encouraging Member States to draft "Code of Conducts" addressed to specific sectors.[442] This tenuous self-regulated approach could become a valuable, alternative tool, serving as a starting point in order to balance the conflictive interest of omnibus regulation and market-driven ideas strongly supported by Europe and the United States respectively.[443] The next section of this chapter will examine the current privacy data legal framework in Canada, assessing its merits and flaws, and the degree of compliance with the stringent requirement of the EC Directive.

4.6. The Canadian Privacy Data Protection Approach

Although playing a lesser role than the United States and Europe in air transport, Canada constitutes a significant player in an industry aiming to implement automation endeavours therein.[444] Thus, a brief review of its privacy data protection legal framework, highlighting its major features becomes mandatory.[445] Canada has formulated a combination approach to the protection of privacy rights, following the US conception on numerous issues, but adopting some European peculiarities.[446] Additionally, the latest Canadian regulation on privacy data protection seeks to balance both conflictive interests, articulating a *suis generis* model.

---

[442] *Ibid.*, art. 27 (1).

[443] Some commentators have expressed that at least in theory the adequacy principle contained in the EC Directive, could be achieved by industry self-regulation methods, such as the implementation of code of conduct. See G. Pearce & N. Platten, "Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective" (1999) 22 Fordham Int'l L. J. 2024 at 2035.

[444] As explained previously in this thesis, Canada is attempting to develop the CANPASS.

[445] This thesis does not attempt to comprehensively analyse the Canadian privacy data scheme. The purpose is solely to identify its major components and uniqueness.

[446] See generally D.H. Flaherty, *Protecting Privacy in Two-Way Electronic Service* (New York: Knowledge Industry Publications, 1985) at 11.

4.6.1. Private and Public Privacy Spheres

As in the United States, the two-fold division of public and private spheres also appears in the Canadian context. The public sphere of privacy data protection, addressing the relationship between individuals and the government, comprises the *Canadian Charter of Rights and Freedoms*,[447] from where the courts have interpreted that two particular sections indirectly address privacy issues. Section 7 provides that "everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice",[448] and Section 8 is the equivalent of the US Fourth Amendment protecting individuals against unreasonable search and seizure.[449] In *Hunter* v. *Southam Inc.*[450] the Supreme Court of Canada acknowledged the existence of the right of privacy as the right to be let alone using the unreasonable search and seizure provision of Section 8 of the Canadian Charter. The court found that the right of privacy "is the right to be secure against encroachment upon the citizens' reasonable expectation of privacy in a free and democratic society".[451] In its decision the court favoured a case-by-case analysis in order to determine whether the law gives a remedy for the invasion of privacy.[452] The court interpreted privacy similarly to the United States examining the individual's "reasonable expectation of privacy" of the individual. Therefore, one can reasonably say that when a case involves privacy infringement by federal government agencies as a result of implementing automation endeavours in air transport, that Canadian courts will tend to apply the reasonable expectation of privacy test, as have their US counterparts. Furthermore, Canada has enacted the *Privacy Data Act*[453] and the *Access to Information Act.* [454] The former governs the collection, use and disclosure of personal information and regulates the conduct of

---

[447] See *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11

[448] See *ibid., Canadian Chapter*, s. 7.

[449] See *ibid., Canadian Chapter*, s. 8.

[450] See *In Canada (Director of Investigation & Research, Combines Investigation Branch)* v. *Southam Inc.* [1984] 2 S.C.R. 145, 27 B.R.L.

[451] See *ibid.*, at 133.

[452] Similar decisions in Canadian courts were held in *Scanne* v. *Orr* (1981), 34 O.R. (2d) 317, 19 C.C.L.T 37 (Co.Ct.); *Lipiec* v. *Borsa* (1996), 31 C.C.L.T. (2d) 294 (Ont. Gen. Div.). The right of privacy has been protected in Canada and the Commonwealth countries under a myriad of different legal theories, *inter alia*, contract, trespass, nuisance, and defamation. See *Green* v. *Minnes* (1891), 22 O.R. 177 (C.A.); *Motherwell* v. *Motherwell* (1976), 73 D.L.R. (3d) 62 [1976] 6 W.W.R (Alta. C.A.); *Robbins* v. *C.B.C.* (1957), 12 D.L.R. (2d) 35, [1958] Que. S.C. 152; *Sim* v. *H.J. Heiz Co. Ltd.*, [1959] 1 W.L.R. 313, [1959] 1 All E.R. 547 (C.A.).

[453] See *Privacy Act*, R.S.C., 1985, c. p-21.s

[454] See *Freedom of Information Act*, R.S.C, 1985, c. a-1

federal agencies with respect to the processing of such data. The latter grants individuals access thereto. Similarly, numerous provinces have adopted privacy legislation.[455] Both the federal government and the provinces can exercise jurisdiction on privacy matters. But perhaps part of the uniqueness of the Canadian privacy data protection legal framework, particularly at the provincial level, stems from the fact that Canada has extended the competence of the Privacy Commission to include not only the provisions dictated by the *Privacy Data Act*, but also to those of the *Access to Information Act*.[456] This watchdog institution plays a significant role in the protection, investigation, enforcement, and mediation of privacy rights in Canada at the provincial and federal level.

4.6.2. The Emergence of a *Suis Generis* model

Hitherto, in respect to the private sphere of privacy data protection Canadians did not have a single comprehensive legislation, but rather sectoral regulation attempting to address specific privacy issues related to certain industries.[457] Had the privacy issue not been contemplated by one of the sectoral legislation enacted, the matter would have been resolved by the tort of privacy in the common law provinces and by statute in the civil law Quebec.[458] The former has faced the same difficulties and shortcomings as the one contained in the United State's system. The latter, following the European example, has adopted the *Act Respecting the Protection of Personal Information in the Private Sector*,[459] which extended the application of privacy data protection to the processing performed by government agencies,

---

[455] See *Privacy Act*, R.S.B.C., 1996, c. c-3736 (British Columbia); *Privacy Act*, R.S.M., 1987, c. p-125 (Manitoba); *Privacy Act*, R.S.N., 1990, c. p-22 (Newfoundland); *Privacy Act*, R.S.S., 1978, c. p-24

[456] See D.H. Flaherty, "Some Reflections on Privacy and Technology" (1999) 26 Man. L.J. 219 at 22.

[457] See *Telecommunications Act*, R.S.C., 1993, c. t-3.4, 39 & 41; *Bank Act*, R.S.C., 1991, c. b-101, 242, 244 & 459; *Insurance Companies Act*, R.S.C., 1991, c. i-11.8, 489 & 607; *Trust and Loan Companies Act*, R.S.C., 1991, c. t-19.8, 444; *Pension Plan Act*, R.S.C., 1985, c. c-8, 104.

[458] For a comprehensive study on Canadian common law torts, see J.D.R. Craig, "Invasion of Privacy and Charter Values: The Common - Law Tort Awakens" (1997) 42 McGill L.J. 355. For Quebec civil law privacy data protection, see K. Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations* (Montreal: Thémis, 1992) at 92; P.A. Comeau & A. Quimet, "Freedom of Information and Privacy: Quebec's Innovative Role in North America" (1995) 80 Iowa L. Rev. 651; H.P. Glenn, "The Right to Privacy in Quebec Law" in D. Gibson, ed., *Aspects of Privacy Law* (Toronto: Butterworths, 1980) at 41. R. Laperrière, "The Quebec Model of Data Protection: A Compromise between *Laissez-Faire* and Public Control in a Technological Era" in C. J. Bennett & R. Grant, eds., *Visions of Privacy – Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) at 182. See also I.B. Lawson, *Privacy and Free Enterprise*, 2d ed. (Ottawa: The Public Interest Advocacy Centre, 1997).

[459] See *Act Respecting the Protecting of Personal Information in the Private Sector*, S.Q., 1993, c.17.

as well as private parties constituting an innovation in North America.[460] This act regulates the collection, use, and disclosure of personal information held by the private entrepreneurial sector operating in Quebec, and grants the individual the right of access to such information. Moreover, Quebec's Civil Code[461] grants the protection and respect of privacy rights. Thus, the legal framework established in Quebec would seem to be the sole one in accordance with the stringent requirement contained in the EC Directive. Some commentators have suggested that the level of privacy protection in Canada offered at the provincial level considerably exceeds that of the federal government with respect to the private sector.[462]

4.6.2.1. The Personal Information Protection and Electronic Documents Act

Canada realised the need of federal legislation to balance the disproportion created by the *Act Respecting the Protection of Personal in the Private Sector* enacted in Quebec with respect to the other provinces, and the fragmented federal regulation or the lack thereof. Consequently, after a long process of negotiations, an agreement was reached in the *Personal Information Protection and Electronic Documents Act*,[463] which was assented on 13 April 2000; it is expected to enter into force progressively as early as 1 January 2001. The novel act comprises two main parts: 1) the protection of personal information; and 2) the regulation of electronic documents as an alternative to the use of paper to record information or transactions.[464] The act seeks to establish rules governing the collection, use, and disclosure of personal information in a manner that balances the right of privacy of all individuals with the need of organisations to collect, use, or disclose personal information[465] for "purposes that a reasonable person would consider appropriate in the circumstances".[466] The foregoing

---

[460] See Comeau & Quimet, *supra* note 458 at 651.
[461] See Articles 35-41 *Civil Code of Quebec* (1993).
[462] See C.J. Bennett, *Implementing Privacy Codes of Practice* (Toronto: Canadian Standards Association, 1995) at 8.
[463] See *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5, s. 2.
[464] See *ibid.*, s. 32.
[465] Personal information is defined in the act as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organisation." See *ibid.*, s. 2(1).
[466] See *ibid.*, s. 3. See also Privacy Commissioner of Canada, "Backgrounder Privacy Provisions Highlights" online: http://strategis.ic.gc.ca/virtual_hosts/e-com/english/fastfacts/43d8.html (date accessed: 28 July 2000). However, the act does not apply to personal information used, collected, or disclosed by an individual for a personal purpose, or by an organisations for journalistic, artistic, literary, or any activity outside of its commercial purpose. See *ibid.*, s.4

represents a magnificent attempt to consider not only the interest of the individual in protecting his privacy rights, but also a remarkable effort not to place an enormous burden on the private entrepreneurial sector. It represents the Canadian general view that favours the adoption of privacy data protection legislation without hindering the normal course of private business. The act was passed only after considering the market factor implications on the private sector. It is the result of a consensus reached among the players involved. In fact, the act was based on the Canadian Standards Association Model Code for the Protection of Personal Information.[467] The latter has been enclosed as "Schedule 1" of the act, aiming at providing the private entrepreneur with guidelines, principles, and suggestions for the development of adequate mechanisms in order to properly safeguard the individuals' personal information.[468] Herein lies one of the main differences from the EC Directive, where the latter was enacted more out of favouritism of the individual's right of privacy, conceived as a fundamental human right, rather than to balance both interests as was done within the Canadian context.

More specifically, the act will enter into force in three different phases: 1) for organisations in the federally regulated private sector, *inter alia*, airlines, telecommunications, banking, broadcasting, and interprovincial transportation, starting on 1 January 2001; 2) health information by 1 January 2002; and 3) full application, commercial use of personal information, whether or not regulated by federal law, on 1 January 2004.[469] The *rationale* of such progressive implementation of the act lies in the fact that certain industry sectors might

---

[467] The Canadian Standards Association has established ten principles for a Model Code for the Protection of Personal Data, including: 1) Accountability Principle, making the organisation responsible for personal information under its control; 2) Identifying Purposes Principle, whereby the intention of collection of such data must be at or before the information is collected to the data subject; 3) Consent and Knowledge Principle, necessary for collection, use or disclosure of personal information; 4) Limiting Use, Disclosure, and Retention Principle, whereby personal information shall only be used for its intended purpose, disclose with the individual's consent, and retain only for the necessary time to comply with its objective, unless otherwise required by law; 5) Accuracy Principle, meaning that personal information must be precise, complete and up-to-date; 7) Security Principle, whereby personal information shall be protected from unwanted intrusion; 8) Openness Principle, whereby the organisation makes available to the individual information about its policies and practices with respect to the handling of personal information; 9) Individual Access Principle, whereby an individual is granted access to the organisation's record of his personal information upon request; and 10) Challenge and Compliance Principle, whereby an individual is capable of challenging the compliance with the aforesaid principles to an specific institution. See *ibid.*, schedule 1. See also Canadian Standards Association, "Model Code for the Protection of Personal Information" online: http://www.csa-international.org/english/product_services/ps_privacy.html (date accessed: 30 July 2000).

[468] See *Personal Information Protection and Electronic Documents Act*, *supra* note 456, schedule 1.

require more time to adopt to the new privacy data requisites. Needless to say, that the act's first phase of implementation will already affect air carriers' common practices and operations, which could have significant consequences in implementing automation initiatives in air transport. One can easily envision numerous practices and procedures that the air transport players might have to re-design in order to comply with the act's requirements.

4.6.2.1.1. The "Reasonable Collection, Usage and Disclosure" Principle

The act denotes that an organisation may collect, use, or disclose personal information solely for "purposes that a reasonable person would consider, are appropriate in the circumstances",[470] establishing the common law long-standing rule of reasoning. It will depend on the Privacy Commissioner and the courts to interpret the legal parameter of "reasonable purposes in appropriate circumstances". The language of the act suggests a slightly different connotation than the one contained in the EC Directive, which makes reference to the collection of data for "specified, explicit and legitimate purposes".[471] The latter has a lesser degree of discretionary spectrum, whereas the former enlarges the act's interpreter *potestas* thereof.

4.6.2.1.2. The "Consent and Knowledge" Principle

The act follows the European principle of data protection, namely that the information cannot be collected or used without the consent of the data subject; but under the Canadian context the latter has been extended to include the individual's consent and knowledge thereto.[472] The purpose of such an extension in the language of the act is to ensure that private organisations make all necessary efforts to reasonably let the data subject

---

[469] See Privacy Commissioner of Canada, "Implementation Schedule" online: http://www.privcom.gc.ca/english/02_06_02a_e.html (date accessed: 29 July 2000).
[470] See *Personal Information Protection and Electronic Documents Act*, S.C., 2000, c. 5, s. 5(3).
[471] See *ibid.*, s. 5(3), comparing *EC Directive*, *supra* note 393, art. 6 (b).
[472] See *ibid.*, schedule 1, c. 4.3.2

know and understand how the information will be handled. Nevertheless, exceptions are provided where the data can be processed without the data subject's consent, for instance, where the collection is clearly in the interest of the individual, where the information is already publicly available, or where the organisation has reasonable grounds to believe that the individual might be contravening Canadian laws.[473] In relation to the air transport context, this means that organisations pursuing to implement automation initiatives must clearly obtain the consent of the data subject and at the same time inform him of the intention of the processing and usage thereof. The preceding will be tantamount to not only meticulous contractual provisions governing the relationship between the air carrier or processing third party, such as a banking institution, and the passenger, but also a substantial modification in the practices and procedures of the aforesaid organisations, ensuring that the data subject fully comprehends the endeavours undertaken with respect to the processing of his personal data. The foregoing discussion could be clearly exemplified where the air carrier offers the issuance of a frequent-flyer smart card with credit card capabilities to the passenger. The airline will have to clarify all the aforesaid issues either at the moment when it reaches the customer by telephone, or when issuing a ticket or a itinerary receipt, the latter being the case of electronic ticketing. Other automation endeavours, such as EDI and API, are also directly triggered by the "consent and knowledge" principle embraced by the Canadian legislation. However, if the extension of the contractual provisions contained in the airline's general conditions of carriage to constitute consent was doubtful within the EC Directive spectrum, the scenario is clearer in the Canadian context. The "consent and knowledge" principle places a much more stringent requirement on the air carrier who has not only to obtain the passengers consent, but rather inform him the consequences thereof. Hence, it is obvious that the "camouflaged consent" as contained in the conditions of carriage does not follow the spirit of the act.

This act provides that organisations cannot use the individual's personal information without the knowledge or consent of the data subject, unless required otherwise by law.[474] The data subject can request in writing individual access to the information,[475] and

[473] See *ibid.*, s. 7(1).
[474] See *ibid.*, s. 7(2).
[475] See *ibid.*, s. 8(1). See also *ibid.*, schedule 1, c. 4.9.

the organisation must respond within thirty days of receipt of the request.[476] However, organisations can extend the aforesaid period for another thirty days, provided such request "unreasonably interferes with the activities of the organisation", or where more time is required to convert the data subject's information into an alternative format.[477] The act also provides remedies where an individual's right of privacy is violated, in this case the data subject may file a written complaint with the Privacy Commissioner,[478] and later, once a report has been issued on the matter, may apply to the Court for a hearing.[479] One can easily expect that the preceding requirements will somewhat change the industry players's procedures and practices.

4.6.2.1.3. Transborder Data Flows

Ab initio, the act does not present any significant legal barrier to the transborder flow of personal data, but perhaps in one of its most relevant provisions for the automation initiatives as envisioned in air transport, the act mandates that where personal information is transferred for processing to a third party, organisations must enter into contractual relationships therewith in order to ensure a similar level of privacy protection.[480] The foregoing constitutes a more flexible requirement than the adequacy principle as envisaged within the European legal framework. The latter is based on the "adequacy" principle, which establishes that personal information can only be transferred to third countries that offer the same standard or level of privacy protection. Although exceptions are provided, the foregoing represents the general rule. Whereas in the Canadian context, the act provides an alternative mechanism such as the adoption of contractual provisions by the parties, instead of directly restricting the flow of personal data as done by the EC Directive.

---

[476] See *ibid.*, s. 8(3).
[477] See *ibid.*, s. 8(4).
[478] See *ibid.*, s. 11. The Commissioner may even conduct audits of the practices of certain organisations where he has reasonable grounds to believe that such enterprise may be contravening the provisions of the act. See *ibid.*, s. 18(1). Similarly, the act contains a whistleblowing provision, whereby any person who has reasonable grounds to believe that a person or an organisation has infringed the act may notify the Commissioner. See *ibid.*, s. 27.
[479] See *ibid.*, s. 14. The court could order the organisation to correct its practices and procedures, or even award damages to the plaintiff. See *ibid.*, s.16.
[480] See *ibid.*, schedule 1, c. 4.1.3.

The spirit of this act seeks to avoid creating insuperable legal hurdles to the entrepreneurial sector, characterising the long-awaited combination of legal regulation and business self-participation. The private sector's initiatives become of paramount importance in the proper development of the system, which are carefully observed by government authorities from "arm's length" distance. One can certainly envisage a large number of contractual provisions governing the relationships of diverse players when implementing automation initiatives in air transport. For instance, Air Canada will be particularly keen on drafting thorough contractual provisions to govern its contractual relationship with those enterprises handling the personal information of the airline's passengers frequent flyer smart cards, as is the case of banking institutions. Another relevant provision of the act refers to the safeguards necessary to guarantee the security of personal information; it establishes that organisations should include: 1) physical measures, such as restricting access to the office; 2) organisational undertakings, whereby the access to sensitive information is restricted according to the "need to know" principle; and 3) technological measures favouring the use of passwords and encryption.[481] These principle are absolutely applicable to all the automation endeavours herein envisioned, and they could certainly represent a valuable tool to avoid any information leaks in the system, which as explained before could have awful consequences for the individuals' right of privacy, particularly taking into account the large amounts of data involved.

4.6.3. Critical Assessment

Although by no means a legal panacea this Canadian act represents an attractive approach to the issue of privacy data protection, essentially because it has been born from the consensus view of regulators, industry players and privacy organisation groups. This thesis supports the argument that the Canadian privacy data protection with the latest enactment of the *Personal Information Protection and Electronic Act* is in accordance with the strict requirements established in the EC Directive. Consequently, issues of transborder data flows are most likely not to occur between the two parties.

[481] See *ibid.*, schedule 1, c. 4.7.3.

Unarguably, the act fails to respond to several issues presented by the implementation of automation in air transport, but the sole fact that the act *ab initio* does not intend to impede the free flow of transfer of information constitutes a major achievement. The act strongly encourages the adoption of alternative mechanisms by means of contractual provisions as well as the implementation of the long-awaited model code on data protection. Bearing in mind the internationalised environment where the air transport initiatives are taken place, it is also uncertain how the courts will interpret the act when call upon privacy claims of foreign individuals.

Notwithstanding the Canadian achievement on regulating privacy data protection, the situation in numerous other countries around the globe, where no clear level of consensus has been achieved yet, creates a somewhat unpredictable scenario for the proper development of automation initiatives in air transport, if such a concern to protect the individual's right of privacy exists.[482]

4.7. The Conflict over Privacy Data Protection Ideologies: Insuperable Legal Hurdles for Transborder Data Flows?

The European ideology of privacy data protection is deeply rooted in the conceptualisation of privacy as a fundamental human right, which must be adequately

[482] The development, level, and mechanism of privacy data protection worldwide varies enormously. Some countries have included specific constitutional provisions guaranteeing the right of privacy to the individual. Moreover, some countries favour the application of these constitutional provisions solely against the government, whereas others favour its further extension to include claims of private parties against themselves. See *Constitution Act Constitutional Act, 1994* (Argentina), arts. 18, 19 & 43; *Constitutional Act* (Paraguay), art. 33; *Commonwealth of Australia Constitutional Act,* 1990; *Constitutional Act, 1988* (Brazil), art. 5; *Constitutional Act, 1991* (Bulgaria), arts. 32, 33 & 40; *Constitutional Act, 1980* (Chile); *Constitutional Act, 1948* (Republic of South Korea) art. 16; *Constitutional Act, 1982* (Turkey), s. 5; *Constitutional Act, 1996* (South Africa) c.2, s. 14. By adopting constitutional provisions too, other countries have primarily focused on the protection of the secrecy of communication, whereby the inviolability of postal documentation is guaranteed. The concept of privacy has been extended to comprise other areas and dimensions. See *Constitutional Act, 1874* (Switzerland), art. 36; *Constitutional Act, 1917* (Mexico), art. 16. Other countries such as China have had a long tradition of weak protection of privacy rights. For a comprehensive assessment of the different legal mechanisms enacted for the protection of privacy worldwide, see D. Banisar & S. Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, and Surveillance Laws and Developments" (1999) 18 J. Marshall J. Computer & Info. L. 1. See also J.B. Rivarola Paoli, *Derecho de la Información* (Asunción, Paraguay: Intercontinental Editora, 1995) at 107; M. Zavala De Gonzalez, *El Derecho a la Intimidad* (Buenos Aires: Abeledo Perrot, 1982) at 41.

protected within a comprehensive legal framework.[483] Although bearing in mind the tremendous European achievement in empowering the data subject with valuable rights and clarifying several areas that still remain unclear in the United States, the main flaw of the European privacy data protection approach lies in the fallacious idea that omnibus legislation will constitute the long-awaited legal panacea, which will be able to confront all the emerging difficulties, brought about by technological advancements. The mere presence of law will not solve the problem. This thesis has shown numerous scenarios where the EC Directive fails to properly respond to the automation initiatives in facilitation of air transport. Moreover, it contains loopholes resulting in obscure confusion. For instance, according to the language of the EC Directive it is doubtful whether the transfer of information by means of EDI as envisaged in Annex 9 would be permitted. Similarly, the electronic transmission of passenger passport data, as conceived in the API system, is rather nebulous. The issue bounces back to the determination of whether the automation initiatives are exempt from the "adequacy principle"; subjective analysis could create endless discussion causing significance economic losses to air transport industry players. On the other hand, the liberal privacy data protection ideology embraced by the United States is based upon the market self-regulation principle embedded in the sectoral legislation, targeting to control at arm's length specific industries. Thus, the privacy data protection in the United States is extremely complex and unpredictable. It is rather uncertain how the US courts will react when being called on to decide on privacy claims related to air transport or any of its automation initiatives, particularly in the private sector. This thesis has outlined numerous deficiencies of the US system in this sector, where the application of the common law tort remedy does not suffice. Furthermore, the American legal system of privacy protection is not in accordance with the stringent European requirements on transfer of data flows.

In fact, none of the aforesaid systems provide a flawless solution to the drastically rising concern of privacy data protection against technological advancements. Ideally, the United States should enact a comprehensive set of privacy data protection legislation to level

[483] One could question to what extent excessive enactment of privacy data protection regulations would create a distortion in the market function, where private enterprises would face adverse circumstances that would eventually put them out of business, increasing the unemployment rate and affecting the economic well-being of the individual. See Posner, *supra* note 268. Notwithstanding the foregoing argument, numerous commentators have expressed that stringent privacy data regulations stimulate consumer participation, particularly in electronic commerce, hence, boosting the overall economy. See Swire & Litan, *supra* note 391 at 86.

up with the European standards, which again are not the legal panacea, but which will ultimately empower individuals to protect their rights. Some commentators have even indicated the advantages of having a Federal Privacy Commission in the United States, an administrative body that would serve as a watchdog of privacy data protection and enforcement thereof.[484] It is unlikely that the United States will comply with the aforesaid requests since that would betray its long-standing capitalistic philosophy. Similarly, the European authorities should adopt more flexible standards, permitting the stronger intervention of industry market-driven ideas. This thesis supports the argument that the US will not enact comprehensive data privacy legislation.[485] Nevertheless, even if it were possible to achieve such utopia of objectives, the latter would not resolve all the problems directly triggering the automation undertakings in air transport, primarily due to the internalisation of the industry,[486] the lager number of players involved, and the rapid development of technological advancements. The adoption of different approaches to the problem herein examined creates a substantive conflict of ideologies, causing a *de facto* barrier for transborder data flows, which is a *sine qua non* requisite for the proper application of automation to air transport endeavours.[487] However, it is indeed worth mentioning that the Canadian approach to privacy data protection seems to suit both the European and American conflictive interest, hence, abolishing any barriers to transfer of data flows. Bearing in mind the foregoing and based upon the Canadian model, this thesis favours the idea of substituting the rigorous "adequacy principle" with a new conceptualisation of transborder data flows, as will comprehensively explained herein.

4.8. An Alternative Proposal to Transborder Data Flows in Air Transport

This thesis strongly supports the argument that the existing privacy data protection framework worldwide does not adequately protect the individual's right of privacy against the

---

[484] See P.M. Schwartz, "European Data Protection Law and Restrictions on International Data Flows" (1995) 80 Iowa L. Rev. 471 at 500. See also Martin, *supra* note 272 at 833.

[485] However, some commentators have said that the United States will be forced to adopt comprehensive data legislation under pressure from enterprises operating in Europe. See H.H. Perritt, Jr., *Law and The Information Superhighway* (New York: Wiley Law Publications, 1996) at 144. For an interesting reference to congressional attempts to create privacy data protection legislation in the United States see Myers, *supra* note 304 at 141.

[486] The air transport environment is by no means of a parochial nature.

[487] For a detailed study on European Transborder of data flows see A.C.M. Nugter, *Transborder Flow of Personal data within the EC* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990).

emerging automation trends in air transport. In addition, the system fails to balance the conflictive interests of the industry players and the data subjects, which is reflected in the barriers to transborder data flows. Needless to say that in order to fully implement automation in facilitation of air transport, privacy data protection legal issues ought to be resolved, whereby the data subject's rights are adequately protected and the air transport industry players' interests are properly balanced therewith. Hence, this thesis attempts to propose a two-fold feasible solution born within the air transport industry, as an alternative response to the privacy concerns, but with the ultimate goal of permitting to implement automation initiatives to facilitate air traffic flows.[488]

First, understanding the complexity of the air transport scenario, where players from the private and public sector interact, this thesis argues for the necessity of further intervention of key government and industry players such as ICAO and IATA. The idea, taken from the CRS Code of Conduct,[489] conceives the development of the "Air Transport Privacy Data Code of Conduct", which would be implemented by international organisations, at the private level and extended if possible to the public sector.[490] The former should be commanded by IATA to establish common personal data handling standards within the airline industry. The latter should be directed by ICAO, who would be in charge of encouraging its Contracting States to adopt the provisions of the code of conduct, and from then on to the administrative agencies dealing with passenger personal data, as is the case of the INS in the United States.[491] It is extremely important that these international organisations join efforts and act together in order to draft a single code of conduct, *contrario*

---

[488] The formulation of a general solution to balance the conflictive interest in privacy data protection dealing with transborder data flows is beyond the scope of this thesis.

[489] See generally R.I.R. Abeyratne, *Legal and regulatory issues of computer reservation systems and code sharing agreements in air transport* (Editions Frontieres, 1995); R.I.R. Abeyratne, "Contractual Liability Arising Out of Computer Reservation systems of Air Transport" (1995) 11:4 Tolley's Computer L. and Practice 97; R.I.R. Abeyratne, "The Display of Airline Computer Reservation Systems on the Internet" (1997) Aviation Q. 360; R.I.R. Abeyratne, "The Trading of Airline Services on the Internet" (1997) 16:5 Trading L. R. 395; M. Wounters, "The Hybrid Relationship Between Computer Reservation Systems (CRSs) and Airlines" (1997) Aviation Q. 346; ICAO, News Release PIO 7/96, "ICAO Council Updates Computer Reservations Systems Code" (June 1996), online: http://www.icao.int/icao/en/nr/pio9607.html (date accessed: 10 August 2000); B. Humphreys, "Computer reservation systems" in J. Pavaux, ed., *Air Transport: Horizon 2020* (Paris: Institut du Transport Aérien, 1995) at 185.

[490] See Gellman, *supra* note 384 at 168 (claiming that when governments are not able to adequately address the issue of international privacy regulation, the private sector may propose other options, such as the adoption and development of voluntary international privacy codes).

[491] This thesis understands the difficulty of imposing the adoption of a code of conduct to national agencies such as the INS in the United States.

sensu, the air transport industry runs the dangerous risk of having several fragmented code of conducts, which might vary in substance and formalities, thus jeopardising the ultimate objective of protecting privacy. The foregoing has been one of the main drawbacks of the CRS model, since numerous different international institutions have formulated code of conducts, *inter alia*, the US Federal Aviation Administration, ICAO, and the European authorities.[492]

The Air Transport Privacy Data Code of Conduct should be drafted on the basis of seven paramount principles: 1) the personal data confidentiality; 2) the adoption of adequate technological measures and infrastructure to ensure security of personal data;[493] 3) the attainment of the data subject's unambiguous consent for the collection, use, and processing of personal data; 4) the notification of the purpose of the collection of personal information to the data subject; 5) the exclusive use of personal data solely for its original intended purpose;[494] 6) the data subject's right to challenge the information;[495] 7) the personal data could only be transferred to third parties provided that a contractual relationship between the parties assures similar levels of data protection. The *rationale* of the foregoing lies in the fact that the principles should create a flexible environment where the individuals' right of privacy is adequately protected, but without extremely onerous costs on the industry sector, hence, permitting the transborder transfer of data flows. By doing so, the air transport industry players will be allowed to develop the automation endeavours, such as MRTDs, API system, SPT and smart cards.

---

[492] See generally EC, *Council Regulation No. 323/1999 of 8 February 1999 amending Regulation (EEC) No. 2299/1989 on a code of conduct for computer reservation systems (CRSs)* [1999] O.J. L. 40/1.

[493] Some commentators have noted that technology plays an important role in protecting privacy rights because it is a viable tool to enhance the individual's right. See S.A. Alpert, "Privacy and Intelligent Highways: Finding the Right Way" (1995) 11 Computer & High Tech. L.J. 97 at 115 (advocating for a technological response to the possible privacy infringement by the implementation of the US Department of Transportation's Intelligent Vehicle Highway Systems).

[494] This is a paramount principle since the interaction of diverse players may create the tendency among them to exchange passenger information as a marketing tool, hence, invading the privacy of individuals.

[495] Another major criticism that could be pronounced at the outset of the formulation of these propositions constitutes the fact that the principles herein promoted could significantly increase the economic cost of the industry players affected thereby. Nevertheless, the Air Transport Privacy Data Code of Conduct pursues to gradually self-adapt the industry players in order to balance state regulation and market driven ideas. Those private industry players not able to meet the demands of legislation and the general public concern on privacy will not be able to compete, hence, they will be driven out of the market. Another flaw of the proposition, especially concerning ICAO, lies in the fact that the proceedings and deliberations of the latter are extremely lengthy and bureaucratic, thereby causing considerable delays to decision making. Nevertheless, ICAO adopts decisions and actions with the consensus of its Contracting States, which eases implementation.

IATA ought to take a leading role in order to encourage the quick adoption of this code of conduct among its members. The industry must promptly respond and adapt itself to the legal hurdles created by legislation such as the EC Directive, and the growing general public concern on privacy. It is in the interest of the industry players to develop the highest degree of customer credibility and reliability on the system, which will eventually be reflected in higher revenues and yields.[496] The foregoing could be substantially achieved by the use of technology, which could fully secure the processing of personal data.[497] Thus, the air transport industry must rapidly balance its interest and the stringent requirements established by regulators such as the European Commission in order to continue doing business as usual. The latter becomes a *sine qua non* requisite.

The foregoing proposition will undoubtedly change the procedures and common practices particularly of the international air carriers dealing with the processing of personal data, thereby slightly favouring the execution of a data subject-oriented policy. The Air Transport Privacy Data Code of Conduct should also include other players that are not part of the industry *per se*, but pursue common interests, such as financial institutions that might be involved in the development of a co-branded frequent flyer smart card with credit card capabilities. Should the intended code not reach the aforesaid players, it would constitute a major flaw in the system, since the levels of personal data processing may considerably

---

[496] This thesis also sustains that a comprehensive economic assessment identifying the cost/benefit of creating a more privacy-reliable environment for data subjects and its direct reflection on the increase of revenues becomes compulsory. See J. Kang, "Information Privacy in Cyberspace Transaction" (1998) 50 Stan. L. Rev. 1193; R.H. McAdams, "The Origin, Development, and Regulation of Norms" (1997) 96 Mich. L. Rev. 425; R.S. Murphy, "Property Rights in Personal Information: An Economic Defence of Privacy" (1996) 84 Geo.L.J.2381; J. Sovern, "Opting In, Opting Out, or No Options at All: The Fight For Control of Personal Information" (1999) 74 Wash. L. Rev. 1033; P.M. Schwartz, "Privacy and the Economics of Personal Health Care Information" (1997) 76 Tex. L. Rev. 1

[497] Some commentators have proposed the adoption of a technological code implemented through machine-to-machine protocols, whereby the individuals are giving the right to choose how the data will be used. See L. Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 162. In a similar vein the European Commission has recognised the importance of developing a technological infrastructure to enhance the level of data protection. See EC, *On-line services and data protection and privacy*, (Annex to the Annual Report 1998, XV D/5047/98 of the Working Party established by Article 29 of Directive 95/46/EC) at 147. For an interesting assessment on information technology security see generally The Canadian Institute of Chartered Accountants, *Information Technology*, 3rd ed. (Toronto: The Canadian Institute of Chartered Accountants, 1998) at 213.

vary.[498] This code of conduct would not only serve to alleviate the conflictive interest created by the stringent requirements of the EC Directive, but also for those industry players located in the United States, the implementation of this idea would create a more data subject-oriented environment where the rights of the individual would be progressively empowered. The latter could have the similar consequences to the enactment of omnibus legislation establishing a data subject's bill of rights; parliamentary action has yet to be taken by the United States Congress.

The preceding discussion could serve as a tool in attempting to resolve some of the privacy data concerns that the implementation of automation in air transport may generate. However, one can envision particularly the European authorities questioning the monitoring and controlling of the proper implementation of such a code of conduct. *De facto*, it is an intricate task to regulate a specific industry when on the other hand self-measures are being encouraged. Thus, an alternative response comes from the industry players' compromise adopting a two-fold contractual approach.[499] First, in all contractual relationships among the industry's private parties involving the implementation of automation endeavours where personal data will be handled, those parties should include contractual provisions underlining the data processing duty of care. Second, the industry players should enter into a contractual relationship with the European authorities in order to grant them the adequate processing of personal data. This alternative has already been conceived as one of the exceptions contemplated in the EC Directive.[500] Most likely, the industry players will be induced to comply with the provisions contained in the contractual relationship because otherwise the

---

[498] One of the strategic objectives pursued with the implementation of the Air Transport Privacy Data Code of Conduct should be to achieve the highest, harmonised standard of personal data processing, ensuring its accuracy and security.

[499] For commentators favouring the adoption a contractual approach to privacy issues, see S.A. Bibas, "A Contractual Approach to Data Privacy" (1994) 17 Harv. J.L. & Pub. Pol'y 591; S. Shorr, "Personal Information Contracts: How To Protect Privacy Without Violating the First Amendment" (1995) 80 Cornell L. Rev. 1756.

[500] See *EC Directive*, *supra* note 393, art. 26 (2). This thesis acknowledges that the solution proposed herein to conciliate the loopholes created by the implementation of automation in facilitation of air transport, is only a patchwork proposition; it does not seek to establish a universal formula. As a matter of fact, some commentators have already indicated that the contractual approach to circumvent the adequacy principle enclosed in the EC Directive could only be applicable where the parties involved have considerable economic strength and level and the endeavours they undertake justifies assuming the risk, a scenario that is not at all familiar to small enterprises. See M.W. Heydrich, "A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract" (1999) 25 Brooklyn J. Int'L L. 407 at 436.

European Authorities will not permit them to operate therein.[501] Nevertheless, one can also question to what extent these alternative propositions guarantee legal remedies to the data subject when his privacy rights are violated.[502]

4.9. Privacy Assessment

In a nutshell, this thesis argues that the consequences of implementing automation in facilitation of air transport will by all means affect the individual's privacy rights, creating a myriad of difficulties and complications. The *rationale* of the foregoing lies in the fact that all initiatives envision the collection of large amounts of passenger data. The quest is then to balance both conflictive interests. Notwithstanding numerous libertarians who have already expressed serious concerns about the development of technological devices that can ultimately create a surveillance environment, where individuals are absolutely traceable, this thesis sustains that the social objective, on behalf of the public interest, pursued by the implementation of automation in facilitation far outweigh the individual's privacy interest. The air transport industry must respond to the rising air traffic growth in the interest of the general public, and indisputably automation constitutes a viable solution.[503] Otherwise passengers could still experience the tortuous consequences of congested immigration queues and overcrowded customs lines. Hence, the public interest will be best served by permitting such intrusive initiatives to succeed, as long as they are observed from arm's length by regulatory authorities, international bodies, or by the industry itself.[504] The latter statement becomes rather mandatory, particularly analysing the utopia of achieving uniform legislation in this respect on a global basis. This thesis thus sustains that the level of involvement and participation of organisations such as ICAO, IATA, and other industry players will most likely determine the degree of success of those initiatives. The formulation

---

[501] One can certainly question to what extent the requirement of a contractual compromise will constitute such an onerous cost of doing business that industry players will eventually opt for abandoning automation endeavours. For a comprehensive study on the impact of the EC Directive, see G. Shafter, "Globalisation and Social Protection: The Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards" (2000) 25 Yale J. Int'l L. 1 at 17.

[502] Another possible flaw of the system may constitute the difficulty of enforceability due to the internalisation of the players involved, issue which can not even be resolved by the enactment of omnibus legislation, as previously explained.

[503] See A. Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999) at 103-137 (asserting, for instance, that non-usage of ID cards and biometric identifiers because of privacy concerns are in numerous cases impractical and considerable costly to society).

[504] See generally P.6, *The Future of Privacy*, vol. 1 (London: Demos, 1998) at 266. V

of an Air Transport Privacy Data Code of Conduct, the establishment of contractual relationships, and the implementation of technology to create a secure environment are highly desirable and recommended.

Conclusion

It has been strongly supported throughout this thesis that air transport is experiencing dramatic, uncontested traffic growth, which is expected to triple in the next 20 years. Therefore, it is mandatory for industry players to somehow reallocate those passengers, since as it has been mentioned previously herein, countries will not have the financial capability to triple the current infrastructure to meet this challenging demand. Hence, implementing automation devices, procedures, and mechanisms will remarkably facilitate passenger clearance at immigration and customs controls. In this respect, it has been indicated that the Chicago Convention sets the background for regulating and co-ordinating initiatives undertaken by Contracting States at the public international level. Furthermore, a critical analysis of Annex 9 has shown its significant role in facilitating passenger flows in air transport. However, the "consensus" nature of ICAO reflects the degree of compromise that States are willing to undertake. Several provisions contained in Annex 9 should have a more stringent language, such as the ones dealing with drug trafficking. The latter, as well as security, are paramount issues that should not be ignored when implementing automation initiatives, because in doing so, the air transport industry could face unwanted consequences.

The prospect of numerous automation endeavours has been carefully examined in this thesis. MRTDs, the API system, smart cards with biometric measurement devices, INSPASS, CANPASS, the SPT, and electronic identity cards offer viable solutions to the emerging traffic growth. Nevertheless, it has been said that such accomplishment is somewhat partial and fragmented due to the disparity of technical and legal standards presented by very dissimilar groups of industry players. The difference of economic strength between the developed and developing world constitute an insuperable hurdle for the global implementation of those initiatives. Moreover, hitherto, only an elite group of frequent-flyers have been targeted.

It has been indicated that a myriad of different legal issues are engaged by these activities. Special attention has been given to some relevant financial, consumer, and

evidentiary issues. The experience of credit and debit cards with unauthorised uses could serve as a valuable example when constructing the system infrastructure of especially the SPT. Issues of inadmissible passengers may also occur once the initiative achieves a larger degree of development, thereby triggering some provisions of Annex 9. The judicial response to the acceptance of computer-generated records remains to be seen in those countries where the legal system is not yet ready to accommodate such quest.

The legal analysis of this thesis has been primordially concentrated on the subject of privacy. Bearing in mind the threat of invading the individual's right of privacy that these endeavours create, this thesis has strongly supported the idea that the public interest pursued therein outweighs the data subject's privacy interest.

Three legal systems and their prominent features have been analysed, especially taking into account where the air transport's largest markets are situated. The first comprises the legal framework of the United States and its industry-driven ideology characterised by self-regulation measures. The second consists of the privacy data protection model presented by the EC Directive, attempting to establish omnibus legislation. The third one constitutes the Canadian approach to privacy, aimed at balancing the conflictive interest between data subjects and data users. None of the foregoing offers flawless privacy solutions to the emerging phenomena of automation in air transport. The industry *per se* is an internationalised environment where balkanised players interact. Hence, very rarely the enactment of legislation will answer all the questions these initiatives raise. Therefore, this thesis has proposed the formulation of an Air Transport Privacy Data Code of Conduct as an alternative response to reconcile such different ideologies. The code of conduct attempts to achieve the longed-for equilibrium between the needs of industry players and the privacy concerns of individuals, a *sine qua non* condition to fully implement automation in air transport. However, such should be carefully observed by government authorities at an arm's length. The degree of success of the code of conduct will significantly rely on the degree of involvement of all the players affected, particularly IATA and ICAO, who ought to lead the torch towards a balanced air transport environment.

Bibliography
Table of Conventions & Resolutions
(in order of signature)

1. *Convention on the International Civil Aviation*, 7 December 1944, 15 U.N.T.S. 295, ICAO Doc. 7300/6.
2. *Universal Declaration of Human Rights*, GA Res. 217(III), 10 December 1948.
3. *American Declaration on the Rights and Duties of the Man* (1948).
4. *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S.5.
5. *International Covenant on Civil and Political Rights*, GA Res. 2200 (XXI), 16 December 1966, art. 17.
6. *American Convention on Human Rights*, 22 November 1969, San Jose, Costa Rica.
7. *Convention establishing the Organisation for Economic Co-operation and Development*, 14 December 1960, Paris, France.
8. Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, Europ. T.S. No. 108 (28 January 1981).
9. *Declaration of the International Conference on Drug Abuse and Illicit Trafficking and Comprehensive Multidisciplinary Outline of Future Activities in Drug Abuse Control*, U.N. Doc. StT/NAR/14, U.N. Sales No. E.88 XI (1988).
10. *United Nations Convention on Protection of the Child*, GA Res. 44/25, 12 December 1989.
11. *Draft Guidelines for the regulation of computerised personal data files*, GA Res. 1989/44, 44th Sess. (15 December 1989).
12. *Guidelines for the regulation of computerised personal data files*, GA Res. 45/95, 68th Plenary Sess. (14 December 1990).
13. *United Nations Convention on Migrant Workers*, A/RES/45/158, 25 February 1991.

ICAO Resolutions, Documents & Studies

(in chronological order)

1. ICAO, *Co-ordination of activities between the United Nations and ICAO relating to emergency action to assist in the maintenance of international peace and security*, Assembly Resolution A5-5, online: http://www.icao.int/icao/en/res/a5_5.html (date accessed: 23 August 2000).
2. ICAO, *Machine Readable Passport*, ICAO Doc. 9303 Part 1, 1st ed. (1980).
3. ICAO, *Security Manual for Safeguarding Civil Aviation Acts of Unlawful Interference*, ICAO Doc. 8973/3 (1987).
4. ICAO, *The Drug Problem*, ICAO Doc. AN-WP/5918.
5. ICAO, *Role of ICAO in the suppression of illicit transport of narcotic drugs by air*, Assembly Resolution A27/12 (October 1989), online: http://www.icao.int/icao/en/res/a27_12.html (date accessed: 15 August 2000).
6. ICAO, *Machine Readable Travel Documents - Machine Readable Visas*, ICAO Doc. 9303 Part 2, 2nd ed. (1994).
7. ICAO, *Outlook for Air Transport to the Year 2003* (Montreal: ICAO, 1995).
8. ICAO, News Release PIO 4/95, "ICAO Facilitation Meeting Considers Aircraft Disinsection, Public Health, Asylum Seekers and Persons with Disabilities" (April 1995), online: http://www.icao.int/icao/en/nr/pio9504.html (date accessed: 9 July 2000).
9. ICAO, *Investment Requirements of Aircraft Fleets and for Airport and Route Facility Infrastructure to he Year 2010* (Montreal: ICAO, 1995).
10. ICAO, *Machine Readable Travel Documents - Size 1 and Size 2 Machine Readable Official Travel Documents*, ICAO Doc. 9303 Part 3, 1st ed. (1996).
11. ICAO, News Release PIO 7/96, "ICAO Council Updates Computer Reservations Systems Code" (June 1996), online: http://www.icao.int/icao/en/nr/pio9607.html (date accessed: 10 August 2000).
12. Annex 9 (Security) to the *Convention on International Civil Aviation*, 6th ed. (March 1997).
13. Annex 9 (Facilitation) to the *Convention on International Civil Aviation*, 10th ed. (April 1997).
14. ICAO, *Consolidated statement of ICAO continuing policies and associated practices related specifically to air navigation*, Assembly Resolution A32-14, Appendix A (October, 1998).
15. ICAO, *Establishment of an ICAO universal safety oversight audit programme*, Assembly Resolution A32-11 (1998), online: http://www.icao.int/icao/en/res/a32_11.html (date accessed: 24 August 2000).
16. ICAO, *Consolidated statement of continuing ICAO policies in the air transport field*, Assembly Resolution A32-17, Appendix D (October, 1998), online: http://www.icao.int/icao/en/res/a32_17.html (date accessed: 23 August 2000).
17. ICAO, *International co-operation in protecting the security and integrity of passports*, Assembly Resolution A32-18 (1998) online: http://www.icao.int/icao/en/res/a32_18.html (date accessed: 26 June 2000).
18. ICAO, *Aims and Objectives of ICAO in the Field of Facilitation*, ICAO Doc. 7891-C/908.
19. ICAO, *Request for information – Biometric recording and verification technologies, machine verification technologies and document security devices*, WP/9 presented at TAG-MRTD/10, 18-20 February 1998.

20. ICAO, *Amendment to informative annex on machine assisted document security verification*, WP/8 presented at TAG-RT/11; 1-3 September 1999.
21. ICAO, *Enhancement of specifications of displayed feature(s) on MRTDs*, WP/10, presented at TAG-MRTD/11, 1-3 September 1999.
22. ICAO, *Supplemental edition to Annex 9*, forthcoming in November 2000.

European Union Documents & Studies

(in chronological order)

1. EC, *Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Strasbourg, 1981).
2. EC, *Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*, [1981] O.J. L. 246/31.
3. EC, *Protection of personal data used for social security purposes* (Strasbourg, 1986).
4. EC, *New technologies: a challenge to privacy protection?* (Strasbourg, 1989).
5. EC, *Council Decision of 31 March 1992 in the field of security of information systems* [1992] O.J. L.123/19.
6. EC, *Directive 95/46 EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L. 281/31.
7. See EC, *Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange*, [1994] O.J. L. 338/98.
8. EC, *Handbook on cost-effective compliance with Directive 95/46/EC*, (Annex to the Annual report 1998 of the working party established by Article 29 of Directive 95/46/EC).
9. EC, *The feasibility of a seamless system of data protection rules for the European Union*, (Study Contract ETD/95/B5-3000/MI/169) by Douwe Korff (Contractor, 1998).
10. EC, *On-line services and data protection and privacy*, (Annex to the Annual Report 1998, XV D/5047/98 of the Working Party established by Article 29 of Directive 95/46/EC).
11. EC, *Council Regulation No. 323/1999 of 8 February 1999 amending Regulation (EEC) No. 2299/1989 on a code of conduct for computer reservation systems (CRSs)* [1999] O.J. L. 40/1.

Other Documents and Reports

1. IATA, *General Conditions Of Carriage*, Recommended Practice 1724.
2. ISO, *Identification Cards – Machine Readable Travel Documents – Part 1: Machine Readable Passport*, Doc. 7501, 3rd ed. (1997).
3. ISO, *Identification Cards - Machine Readable Travel Documents - Part 2: Machine Readable Visa*, Doc. 7501-2, 2nd ed. (1997).
4. ISO, *Identification Cards – Machine Readable Travel Documents – Part 3: Machine Readable Official Travel Documents*, ISO 7501-3 1st ed. (1997).
5. UNCITRAL, "Legal Value of Computer Records" A/CN.9/265, 21/2/1985.

Table of Legislative Instruments
(in alphabetical order)

Argentina

1. *Constitutional Act, 1994.*

Australia

1. *Commonwealth of Australia Constitutional Act*, 1990.

Brazil

1. *Constitutional Act, 1988.*

Bulgaria

1. *Constitutional Act, 1991.*

Canada

1. *Act Respecting the Protecting of Personal Information in the Private Sector*, S.Q., 1993.
2. *Bank Act*, R.S.C., 1991.
3. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (U.K.), 1982.
4. *Civil Code of Quebec* (1993).
5. *Freedom of Information Act*, R.S.C, 1985.
6. *Insurance Companies Act*, R.S.C., 1991.
7. *Pension Plan Act*, R.S.C., 1985.
8. *Personal Information Protection and Electronic Documents Act*, S.C., 2000.
9. *Privacy Act*, R.S.C., 1985.
10. *Privacy Act*, R.S.B.C., 1996, (British Columbia).
11. *Privacy Act*, R.S.M., 1987, (Manitoba).
12. *Privacy Act*, R.S.N., 1990, (Newfoundland).
13. *Privacy Act*, R.S.S., 1978.
14. *Telecommunications Act*, R.S.C., 1993.
15. *Trust and Loan Companies Act*, R.S.C., 1991.

Chile

1. *Constitutional Act, 1981.*

Colombia

1. *Constitutional Act, 1991.*

Finland

1. *Act on Electronic Service in the Administration*, 1999 online: http://www.edita.fi/sk/99/vihko159.pdf (date accessed: 22 August 2000).
2. *The Identity Card Act*, 1999, online: http://www.edita.fi/sk (date accessed: 22 August 2000).
3. *The Population Information Act*, Law 503, 1993 as amended by Law 527 in 1997 online: http://www.edita.fi/sk (date accessed: 22 August 2000). See also *The Population Information Decree*, 886 of 1993.
4. *Personal Data Act*, Law 523, 1999, online: http://www.edita.fi/sk/vuosi99/index.html (date accessed: 22 August 2000).

Mexico

1. *Constitutional Act, 1917.*

Netherlands

1. *Wetbescherming persoonsgegevens*, 1999.

Paraguay

1. *Constitutional Act, 1992.*

Portugal

1. *Constitutional Act, 1976*

Republic of South Korea

1. *Constitutional Act, 1948.*

South Africa

1. *Constitutional Act, 1996.*

Spain

1. *Constitutional Act, 1978.*

Switzerland

1. *Constitutional Act, 1874.*

Turkey

1. *Constitutional Act, 1982*

United States

1. *Cable Communication Policy Act of 1984.*
2. *Credit Card Fraud Act*, 12 C.F.R. 226 (1997).

3. *Fair Credit Reporting Act*, 15 U.S.C. 1681 (1998).
4. *Freedom of Information Act of 1967*, 5 U.S.C. § 552 (1994).
5. *Electronic Communication Privacy Act of 1986*, 18 U.S.C. 2510
6. *Employee Polygraph Protection Act of 1988.*
7. *Identity Theft Prevention Act of 2000*, Bill 2328, 106th Congress
8. *Privacy Act of 1974*, 5 U.S.C. § 552a.
9. *Restatement (First) of Torts* (1939).
10. *Restatement (Second) of Torts* § 652 (1977).
11. *Right to Financial Privacy*, 12 U.S.C. 3401.
12. *Social Security Act*, 42 U.S.C. 301-1011.
13. *Telemarketing Protections Act of 1991.*
14. *The Electronic Fund Transfer Act of 1978*, 12 C.F.R. 205.
15. United States, *Constitution.*
16. *United States Customs Regulations*, 19 C.F.R. § 122.48
17. *Video Privacy Protection Act of 1988*,

Table of Cases
(in alphabetical order)

Canada

1. *Green* v. *Mimnes* (1891), 22 O.R. 177 (C.A.).
2. *In Canada (Director of Investigation & Research, Combines Investigation Branch)* v. *Southam Inc.* [1984] 2 S.C.R. 145, 27 B.R.L.
3. *Lipiec* v. *Borsa* (1996), 31 C.C.L.T. (2d) 294 (Ont. Gen. Div.)
4. *Motherwell* v. *Motherwell* (1976), 73 D.L.R. (3d) 62 [1976] 6 W.W.R (Alta. C.A.).
5. *Scarne* v. *Orr* (1981), 34 O.R. (2d) 317, 19 C.C.L.T 37 (Co.Ct.).
6. *Sim* v. *H.J. Heiz Co. Ltd.*, [1959] 1 W.L.R. 313, [1959] 1 All E.R. 547 (C.A.
7. *Robbins* v. *C.B.C.* (1957), 12 D.L.R. (2d) 35, [1958] Que. S.C. 152.

International Court of Justice

1. *Libyan Arab Jamahiriya* v. *United Kingdom.*
2. *Libyan Arab Jamahiriya* v. *United States of America*

Sweden

1. Decision of the Administrative Court of Appeals, Stockholm, Case No. 2104-1996 (23 April 1997).

United States

1. *Alaska* v. *Morgan*, 985 P.2d 1022 (Alas. App. 1999).
2. *Albright* v. *United States*, 732 F.2d 181 (D.C. Cir. 1984).
3. *American Federation of Government Employees* v. *U.S. Railroad Retirement Board*, 742 F. Supp. 450 (N.D. Ill. 1990).
4. *Arthur* v. *Department of Soc. & Health Servs.*, 576 P.2d 921 (Wash. Ct. App. 1978).
5. *Ault* v. *Hustler Magazine, Inc.* 860 F.2d 877 (9th Cir. 1988).
6. *Berlin Democratic Club* v. *Rumsfeld*, 410 F. Supp. 144, (DC Dist. Col, 1976).
7. *Berger* v. *New York*, 388 U.S. 41 (1967).
8. *Bond* v. *United States*, 120 S. Ct. 1462 (2000).
9. *California* (State of) v. *Ciraolo*, 476 U.S. 207 (1986).
10. *Chambers* v. *Klein*, 564 F. 2d 89 (3d Cir. 1977).
11. *Conant* v. *Hill*, 326 F. Supp. 25 (E.D. Va. 1971).
12. *Cox Broadcasting* v. *Cohn*, 420 U.S. 469 (1979).
13. *DOJ* v. *Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).
14. *Fitzpatrick* v. *Internal Revenue Service*, 665 F.2d 327 (11th Cir. 1982).
15. *Fontan de Maldonado* v. *Lineas Aereas Costarricenses S.A.*, 936 F.2d. 630 (1st Cir. 1991).
16. *Goldman* v. *United States*, 316 U.S. 129 (1942).
17. *Griswold* v. *Connecticut* 381 U.S. 479 (1965).
18. *Jacobson* v. *Rose* 592 F.2d 515 (CA9 Nev., 1978).
19. *Kansas (State of)* v. *Howard*, 221 Kan. 51, 557 P.2d 1280 (Kan. 196).

20. *Katz* v. *United States*, 389 U.S. 347 (1967).
21. *Kimberlin* v. *United States Dept. of Justice*, 788 F.2d 434 (CA7 111, 1986).
22. *Iacobucci* v. *Newport (City of)*, 785 F.2d 1354 (6th Cir. 1986).
23. *Lisi* v. *Alitalia*, 370 F. 2d 508 (3d Cir. 1966).
24. *Lopez* v. *United States*, 373 U.S. 427 (1963).
25. *Miller* v. *New York Stock Exchange*, 425 F.2d 1074 (2d Cir. 1970).
26. *Olmstead* v. *United States*, 277 U.S. 438, 478 (1928).
27. *Pavesich* v. *New England Life Insurance Co.*, 122 Ga. 190, 50 S.E 68 (1905).
28. *Perkey* v. *Department of Motor Vehicles*, 42 Cal. 3d 185 (1986).
29. *Peterson* v. *Arkansas (State of)*, 326 Ark. 1004, 935 S.W. 2d 266, 267 (Ark. 1996).
30. *Prudential Insurance Co.* v. *Cheek*, 259 U.S. 530 at 543 (1922).
31. *Roberson* v. *Rochester Folding Box Co.*, 171 N.Y. 538 at 564 (Super. Ct. N.Y. City 1893).
32. *Ray* v. *Department of Justice*, 720 F.2d 216 (D.C. Cir. 1983).
33. *Roe* v. *Wade*, 410 U.S. 113 (1973).
34. *Sidis* v. *F-R Publishing Corp.*, 113 F.2d 808 (2nd Cir. 1940).
35. *Silverman* v. *United States*, 365 U.S. 505 (1961).
36. *Skinner* v. *Railway Labour Executives Association*, 489 U.S. 602 (1989).
37. *Smith* v. *Maryland (State of)*, 442 U.S. 735 (1979).
38. *Stowe* v. *Devoy*, 588 F.2d 336 (CA2 NY, 1978).
39. *Terry* v. *Ohio*, 392 U.S. 1 at 9 (1968).
40. *Thomas* v. *United States Dept. of Energy*, 719 F.2d 342 (1983).
41. *Thorn* v. *New York Stock Exchange*, 306 F. Supp. 1002 (S.D.N.Y. 1969).
42. *United States* v. *Smith*, 91-5077 (5th Cir. 1992).
43. *United States* v. *Cotroni*, 527 F.2d 708 (CA2 NY., 1975).
44. *United States* v. *Toscanino*, 500 F.2d 267, (CA2 NY, 1974).
45. *United States* v. *Delaplane*, 479 U.S. 827 (1986).
46. *United States* v. *Bennet*, 410 F. Supp. 144 (DC Puerto Rico, 1982).
47. *United States* v. *Burford*, 755 F. Supp. 607 (SD NY, 1991).
48. *United States* v. *Phillips*, 479 F. Supp. 423 (MD Fla., 1979).
49. *Vernonia* v. *Wanye Acton*, 513 U.S. 1145 (1995).
50. *Voelker* v. *Internal Revenue Service*, 489 F. Supp. 40 (ED Mo., 1980).
51. *Vymetalik* v. *FBI*, 251 App DC 402 (1986).
52. *Whalen* v. *Roe*, 429 U.S. 589 (1977).
53. *Washington (State of)* v. *Jefferson*, 11 Wn. App. 745; 524 P.2d 924 (Wash. 1974).

Books, Monographs & Dictionaries

(in alphabetical order)

1. Abeyratne, R.I.R., *Legal and regulatory issues of computer reservation systems and code sharing agreements in air transport* (Editions Frontieres, 1995).
2. Abeyratne, R.I.R., *Aviation Security: Legal and Regulatory Aspects*, 1st ed. (Brookfield, Vermont: Ashgate, 1998).
3. Antieau, C.J., *Modern Constitutional Law*, vol. I (San Francisco: Brancroft Whitney Company, 1969).
4. Aronstam, P., *Consumer Protection, Freedom of Contract and the Law* (Cape Town: Juta & Company, 1979).
5. Auriemma, M.J. & Coley, R.S., *Bankcard Business* (Washington: American Bankers Association, 1992).
6. Benyekhlef, K., *La protection de la vie privée dans les échanges internationaux d'informations* (Montreal: Thémis, 1992).
7. Bennett, C.J., *Implementing Privacy Codes of Practice* (Toronto: Canadian Standards Association, 1995).
8. Bennet, C.J., *Regulating Privacy* (Ithaca, New York: Cornell University Press, 1992).
9. *Black's Law Dictionary*, 7th ed. (St. Paul, Minnesota: West, 1999).
10. Braverman, B.A. & Chetwynd, F.J., *Information Law*, vol.1 (New York: Practising Law Institute, 1985).
11. Buergenthal, T., *Law Making in the International Civil Aviation Organisation* (Syracuse, New York: Syracuse University Press, 1969).
12. Burnham, D., *The Rise of the Computer State* (New York: Random House, 1983).
13. Button, K., ed., *Airline Deregulation, International Experiences* (New York: New York University Press, 1991).
14. Casey, Jr., W.L., Marthinsen, J.L. & Moss, L.S, *Entrepreneurship, Productivity, and the Freedom of Information Act* (Lexington, Massachusetts: Lexington Books, 1983).
15. Cate, F.H., *Privacy in the Information Age* (Washington, DC: Brookings Institution Press, 1997).
16. Cheng, B., *Studies in International Space Law* (Oxford: Claredon Press, 1997).
17. Chorafas, D.N., *Electronic Funds Transfer* (London: Butterworths, 1988).
18. Cooley, T.M., *A Treatise on the Law of Torts*, 2nd ed. (Chicago: Callaghan, 1888).
19. Doganis, R., *Flying Off Course* (London: Routledge, 1991).
20. Drury, T. & Ferrier, C.W., *Credit Cards* (London: Butterworths, 1984).
21. Eaton, J.W., *Card-Carrying Americans* (Totowa, New Jersey: Rowman & Littfefield Publishers, 1986).
22. Erns, M.L. & Schwartz, A.U., *Privacy - The Right to Be Let Alone* (New York: McMillan, 1962).
23. Etzioni, A., *The Limits of Privacy* (New York: Basic Books, 1999).
24. ICAO, *The Convention on International Civil Aviation. Annexes 1 to 18* (Montreal: ICAO, 1991).
25. Evans, D.S. & Schmalensee, R., *Playing with Plastic* (Cambridge, Massachusetts: The MIT Press, 1999).
26. Farnsworth, E.A., *Farnsworth on Contracts*, 2nd ed., vol. 1 (New York: Aspen Law & Business, 1998).

27. Flaherty, D.H., *Privacy in Colonial New England* (Charlottesville: University Press of Virginia, 1972).
28. Flaherty, D.H., *Privacy and Government Data Banks* (London: Mansell, 1979)
29. Flaherty, D.H., *Protecting Privacy in Two-Way Electronic Service* (New York: Knowledge Industry Publications, 1985).
30. Flaherty, D.H., *Protecting Privacy in Surveillance Societies* (Chapel Hill, North Carolina: The University of North Carolina Press, 1989).
31. Franklin, J.D. & Bouchard, R.E., eds., *Guidebook to the Freedom of Information and Privacy Acts*, vol. 1, 2nd ed. (New York: Clark Boardman Callaghan, 1995).
32. Furmston, M., Gakuin, K. & Poole, J., *Contract Formation and Letters of Intent* (Chichester, England: John Wiley & Sons, 1998).
33. Halpin, A., *Rights & Law Analysis & Theory* (Oxford: Hart Publishing, 1997).
34. Harris, L., & Westin, A.F., *The Dimensions of Privacy* (New York: Garland Publishing, 1981).
35. Heuston, R.F.V & Buckley, R.A., *Salmond & Heuston on the Law of Torts*, 20th ed. (London: Sweet & Maxwell, 1992).
36. Hoffer, S., *World Cyberspace Law* (Juris Publishing, 2000)
37. Jain, L.C., Halici, U., & Hayashi, I., eds., *Intelligent Biometric Techniques in Fingerprint and Face Recognition* (Portland: Press International Series on Computational Intelligence, 1999).
38. J. Montgomery Curtis Memorial Seminar, *The Public, Privacy and the Press: Have the Media Gone Too Far?* (American Press Institute, 1992).
39. Johnston, D., Johnston, D. & Handa, S., *Understanding the Information Highway* (Toronto: Stoddart Publishing, 1995).
40. Keeton, P.W., ed., *Prosser and Keeton on Torts*, 5th ed. (St. Paul, Minnesota: West Publishing, 1984).
41. Kirkman, P., *Electronic Funds Transfer Systems* (Oxford: Basil Blackwell, 1987).
42. Konicek, J. & Little, K., *Security, ID Systems and Locks*, (Boston: Butterworth-Heinemann, 1997).
43. Kuhn, T., *The Structure of Scientific Revolution*, 3rd. ed. (Chicago: University of Chicago Press, 1996).
44. Lake, R.B. & Draetta, U., *Letter of Intent and Other Precontractual Documents* (Stoneham, Massachusetts: Butterworth Legal Publishers, 1989).
45. Lessig, L., *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).
46. Lawson, I.B., *Privacy and Free Enterprise*, 2d ed. (Ottawa: The Public Interest Advocacy Centre, 1997).
47. Lipis, H.P., Marschall, T.R. & Linker, J.H., *Electronic Banking* (New York: John Wiley & Sons, 1985).
48. Lloyd, I.J., *Information Technology Law* (London: Butterworths, 1997).
49. Liyanage, S.D., *International Airline Code-Sharing* (LL.M. Thesis, McGill University 1996) [unpublished].
50. Lively, D.E., *Landmark Supreme Court Cases* (Wesport, Connecticut: Greenwood Press, 1999).
51. Macdougall, D.V.,Mosley, R.G. & Sanders, G.J.I., *Credit Card Crime in Canada* (Ottawa, Canadian Association of Crown Counsel, 1985).
52. Mackaay, E., Poulin, D. & Trudel, P., eds., *The Electronic Superhighway* (London: Kluwer Law International, 1995).
53. Mandell, L., *Credit Card Use in the United States* (Ann Arbor, Michigan: The University of Michigan Press, 1972).

54. Mandell, L., *The Credit Card Industry* (Boston: Twayne Publishers, 1990).
55. Michael, J., *Privacy and Human Rights* (Hampshire, England: Dartmouth Publishing Company, 1994).
56. Miller, A.R., *The Assault on Privacy* (Ann Arbor, Michigan: The University of Michigan Press, 1971).
57. Moore, R.L., *Mass Communication Law and Ethics* (Mahwah, New Jersey: Lawrence Erlbaum Associates. 1999)
58. Moreno Rufinelli, J.A., *Nuevas Instituciones de la Constitución Nacional* (Asuncion, Paraguay: Intercontinental Editora, 1996).
59. Moreno Rufinelli, J.A., *La Tarjeta de Crédito* (Asunción, Paraguay: Intercontinental Editora, 1994).
60. Mugillo, R.A., *Tarjeta de Crédito* (Buenos Aires: Editorial Astrea, 1994).
61. Nock, S.L., *The Costs of Privacy* (New York: Aldine De Gryter, 1993).
62. Nugter, A.C.M., *Transborder Flow of Personal data within the EC* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990).
63. O'Mahony, M., Peirce, M. & Tewari, H., *Electronic Payment Systems* (Boston: Artech House, 1997).
64. Organisation for Economic Co-operation and Development, *Deregulation and Airline Competition* (Paris: OECD, 1988).
65. Organisation for Economic Co-operation and Development, *The Future of International Air Transport Policy* (Paris: OECD, 1997).
66. Organisation for Economic Co-operation and Development, *Trends in International Migration* (Paris: OECD, 1999).
67. Organisation for Economic Co-operation and Development, *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Doc. No. OECDC 58 Final (1980).
68. Organisation for Economic Co-operation and Development, *Information, Computer, Communication Policy* (Paris: OECD, 1983).
69. Orwell, G., *Nineteen eighty-four* (Oxford: Clarendon Press, 1984).
70. Pember, D.R., *Privacy and the Press* (Seattle: University of Washington Press, 1972).
71. Perritt, H.H., Jr., *Law and The Information Superhighway* (New York: Wiley Law Publications, 1996).
72. Prosser, W.L., *The Law of Torts*, 4th ed. (St. Paul, Minnesota: West Publishing, 1971).
73. Rankl, W., & Effing, W., *Smart Card Handbook*, 2nd ed. (Oregon: Book News, forthcoming in September 2000).
74. Regan, P.M., *Legislating Privacy* (Chapel Hill, North Carolina: The University of North Carolina Press, 1995).
75. Reynoso, D.G., *Sistema de Tarjeta de Crédito* (Buenos Aires: Roberto Guido, 1997).
76. Rigaux, F., et al., *La Vie Privée, une liberté parmi les autres?* (Brussels: Maison Larcier, 1992).
77. Rivarola Paoli, J.B., *Derecho de la Información* (Asunción, Paraguay: Intercontinental Editora, 1995).
78. Rosenoer, J., *Cyber Law* (New York: Springer, 1997).
79. Rule, J., et al., *The Politics of Privacy* (New York: Elsevier, 1980).
80. Sayer, P.E., *Credit Cards and the Law: An Introduction* (London: Fourmat Publishing, 1988).
81. Schwartz, B., *A Commentary on the Constitution of the United States*, vol. I (New York: McMillan Company, 1968).

82. Scott, G.G., *Mind Your Own Business - The Battle for Personal Privacy* (New York: Insight Books, 1995).
83. Seipel, P. ed., *From Data Protection to Knowledge Machines* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990).
84. Sloan, I.J., *The Law and Legislation of Credit Cards: Use and Misuse* (New York: Oceana Publications, 1987).
85. Shattuck, J.H.F., *Rights of Privacy* (Skokie, Illinois: National Textbook Company, 1977).
86. Simmel, A., "Privacy Is Not an Isolated Freedom" in J.R. Pennnock & J.W. Chapman, eds., *Privacy* (New York: Atherton Press, 1971).
87. Solomon, E.H., ed., *Electronic Funds Transfers and Payments: The Public Policy Issues* (Boston: Nihoff Publishing, 1987).
88. Steiner, S.T. & Teixeira, D.B., *Technology in Banking* (Homewood, Illinois: Business One Irwin, 1990).
89. Sterling, J.A.L., *The Data Protection Act 1984,* 2d ed. (Bicester, Oxfordshire: CCD Editions Limited, 1984).
90. St. John, P., *Air Piracy, Airport Security, and International Terrorism* (New York: Quorum Books, 1991).
91. Swire, P.P. & Litan, R.E., *None of Your Business* (Washington, DC: Brookings Institution Press, 1998).
92. Tapper, C., *Computer Law,* 4th ed. (London: Longman, 1989).
93. The Canadian Institute of Chartered Accountants, *Information Technology,* 3rd ed. (Toronto: The Canadian Institute of Chartered Accountants, 1998).
94. Valcin, Y., *L'argent électronique: quitte ou double* (Lac Beauport, Quebec: Atelliers Graphiques Marc Veilleux Inc., 1985).
95. Velu, J., *Le Droit Au Respect De La Vie Privée* (Brussels, Belgium: Presses Universitaires de Namur, 1974).
96. Villegas, C.G., *Compendio jurídico, Técnico y práctico de la actividad bancaria* (Buenos Aires: Editorial Depalma, 1990).
97. Wagner Decew, J., *In Pursuit of Privacy* (Ithaca, New York: Cornell University Press, 1997).
98. Wacks, R., *Personal Information* (Oxford: Clarndon Press, 1989).
99. Williams, G. *The Airline Industry and the Impact of Deregulation* (Brookfield, Vermont: Ashgate, 1993).
100. Westin, A., *Privacy and Freedom* (New York: Atheneum, 1967).
101. Zavala De Gonzalez, M., *El Derecho a la Intimidad* (Buenos Aires, Argentina: Abeledo Perrot, 1982).
102. Zelermyer, W., *Invasion of Privacy* (Syracuse: Syracuse University Press, 1959).
103. 6, P., Lasky, K. & Fletcher, A., *The Future of Privacy,* Vol. 2 (London: Demos, 1998).
104. 6, P. *The Future of Privacy,* Vol. 1 (London: Demos, 1998).

Articles

(in alphabetical order)

1. Abeyratne, R.I.R, "The Latin American initiative towards funding the CNS/ATM system" (1998) 2 Aviation Q.151.
2. Abeyratne, R.I.R., "The Proposed International Aeronautical Monetary Fund - Legal and Practical Implications" (1998) 3:1 J. Air Transportation World Wide 1.
3. Abeyratne, R.I.R., "Facilitation and the ICAO Role - A Prologue for the Nineties" (1990) XV Ann. Air & Sp. L. 3.
4. Abeyratne, R.I.R., "Contractual Liability Arising Out of Computer Reservation systems of Air Transport" (1995) 11:4 Tolley's Computer L. and Practice 97.
5. Abeyratne, R.I.R., "The Display of Airline Computer Reservation Systems on the Internet" (1997) Aviation Q. 360.
6. Abeyratne, R.I.R., "The Trading of Airline Services on the Internet" (1997) 16:5 Trading L. R. 395.
7. Abeyratne, R.I.R., "Recent Measures Taken by ICAO and the United Nations to Control the Illicit Transportation of Narcotic Drugs by Air" (1998) XXXIII Eur. Transp. L. 321.
8. Abeyratne, R.I.R., "Attempts at Ensuring Peace and Security in International Aviation" (1996) 24:1 Transp. L.J. 27.
9. Abeyratne, R.I.R., "Aerial Piracy and Extended Jurisdiction in Japan" (1984) 33 Int'l & Comp. L.Q. 596.
10. Abeyratne, R.I.R., "Air Carrier Liability and State Responsibility for the Carriage of Inadmissible Persons and Refugees" (1998) 10:4 Int'l J. Refugee L. 675.
11. Abeyratne, R.I.R., "The Automated Screening of Passengers and the Smart Card - Emerging legal Issues" (1998) XXIII:I Air & Sp. L. 3.
12. Abeyratne, R.I.R., "International Responses Related to Aviation Security: A Legal Analysis. Part I" (1996) 45:2 Z.L.W. 119.
13. Abeyratne, R.I.R., "Legal Aspects of Unlawful Interference with International Civil Aviation" (1993) XXVIII:VI Air & Sp. L. 262.
14. Abeyratne, R.I.R., "The Effects of Unlawful Interference With Civil Aviation on World Peace and the Social Order" (1995) 22:3 Transp. L.J. 449.
15. Abeyratne, R.I.R., "Terror in the Skies: Approaches to Controlling Unlawful Interference with Civil Aviation" (1997) 11:2 Int'l J. Polt. Cult. & Soc. 245.
16. Abeyratne, R.I.R., "Some Recommendations for a New Legal and Regulatory Structure for the Management of the Offence of Unlawful Interference with Civil Aviation" (1998) 25:2 Transp. L.J. 115.
17. Abeyratne, R.I.R., "Emerging Trends on Arrest and Detention of Inadmissible Passengers at the Airport" (1998) VII:II The Bar Association Law Journal 21.
18. Abeyratne, R.I.R., "The E-ticket and Trademark Issues of Computerized Airline Ticketing" (2000) 5:2 Tolley's Communications L. 58.
19. Abeyratne, R.I.R., "Auctions on the Internet of Airline Tickets" (1999) 4:1 Tolley's Communications Law 22.
20. Abeyratne, R "The Role of Automation in Facilitation of Air Transport into the 21st Century" (1995) XX:I Ann. Air & Sp. L. 259.

21. Abeyratne, R.I.R., "International Initiatives at Controlling the Illicit Transportation of Narcotic Drugs by Air" (1997) 63:2 J. of Air L. 289;
22. Abeyratne, R.I.R., "Recent Measures Taken by ICAO and the United Nations to Control the Illicit Transportation of Narcotic Drugs by Air" (1998) 33:3 Eur. Transp. L. 321.
23. Abeyratne, R.I.R., "Recipient States' treatment of Inadmissible aliens and Refugees" (1999) 12:4 Int'l J. Politics, Culture & Society 613.
24. Abeyratne, R.I.R., "Some Recent Trends in Evidential Issues on Electronic Data Interchange – The Anglo American Response" (1994) 13:2 Trading L. R. 103.
25. Abeyratne, R.I.R., "The Development of the Machine Readable Passport and Visa and the Legal Rights of the Data Subject" (1992) XVII:II Ann. Air & Sp. L. 1
26. Abeyratne, R.I.R., "Relief Flights and Humanitarian Intervention: Perspectives in International Law" (1995) 44:1 Z.L.W. 3.
27. Abeyratne, R.I.R., "International Initiatives at Controlling the Illicit Transportation of Narcotic Drugs by Air" (1997) 63:1 J. of Air L. 289.
28. Abeyratne, R.I.R., "Proposals and Guidelines for the Carriage of Elderly and Disabled Persons by Air" (1995) 33:3 J. of Travel Research 52.
29. Allen, C. & Kutler, J., "Overview of Smart Cards and the Industry" in C. Allen & W.J. Bar, eds., *Smart Cards* (New York: McGraw-Hill, 1997).
30. Alexander, Y., & Sochor, E., "International Aviation Security Standards" in Y. Alexander & E. Sochor, eds., *Aerial Piracy and Aviation Security* (Netherlands: Martinus Nijhoff, 1990).
31. Alpert, S.A., "Privacy and Intelligent Highways: Finding the Right Way" (1995) 11 Computer & High Tech. L.J. 97
32. Banisar, D. & Davies, S., "Global Trends in Privacy Protection: An International Survey of Privacy, and Surveillance Laws and Developments" (1999) 18 J. Marshall J. Computer & Info. L. 1.
33. Baker-Kelly, B., "United States Immigration: A Wake Up Call!" (1994) 37 How. L.J. 283.
34. Bibas, S.A., "A Contractual Approach to Data Privacy" (1994) 17 Harv. J.L. & Pub. Pol'y 591.
35. Bloustein, E.J., "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U.L. Rev. 962.
36. Boss, A.H., "The International Commercial Use of Electronic Data Interchange and Electronic Communications Technologies" (1991) 46 Bus. Law. 1787.
37. Bovelander, E. & van Renesse, R., "An Introduction to Biometrics" in Knopjes, F. & Lakerman, P.J., eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999) 13.
38. Bradley, P., "Implementing Airline Electronic Ticketing Using Integrated Circuit Cards" (D. Applied Science Thesis, Dublin: Dublin Institute of Technology, 1999)[unpublished].
39. Brenner, M., "Airline Deregulation – A Case Study in Public Policy Failure" (1998) 16 Transp. L.J. 179.
40. Brenner, M., "Rejoinder to Comments by Alfred Kahn" (1988) 17 Transp. L.J. 253.
41. Bruens, A.C., "Melting the Plastic Theories: Advocating the Common Law of Fraud in Credit Card Non-dischargeability Actions under 11 U.S.C 523 (a) (2) (A)" (1997) 50 Vand. L. Rev. 1257.
42. Budnitz, M.E., "Stored Value Cards and The Consumer: The Need for Regulation" (1997) 46 Am. U.L. Rev. 1027.

43. Budnitz, M.E., "Privacy Protection for Consumer Transactions in Electronic Commerce" Why Self-Regulation is Inadequate" (1998) 49 South Carolina L. Rev. 847.
44. Caminer, B.F., "Credit Card Fraud: The Neglected Crime" (1985) 76 J. Crim. L. & Criminology 746.
45. Cate, F.H., "The Changing Face of Privacy Protection in the European Union and the United States" (1999) 33 Ind. L. Rev. 174.
46. Clark, E., "The Law of Electronic Commerce: EDI, Fax, and Email Technology, Proof, and Liability" (1992) 3:1 J.L. & Science 158.
47. Comeau, P.A. & Quimet, A., "Freedom of Information and Privacy: Quebec's Innovative Role in North America" (1995) 80 Iowa L. Rev. 651.
48. Craig, J.D.R., "Invasion of Privacy and Charter Values: The Common - Law Tort Awakens" (1997) 42 McGill L.J. 355.
49. de Groot, A., "Social Risk of Chipcards" in Knopjes, F. & Lakeman, P.J., eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999) 69.
50. Dempsey, P.S., "Airline Deregulation in the United States: Competition, Concentration, and Market Darwinism" (1992) XVII:I Ann. Air & Sp. L. 199.
51. Dinning, M., "Transportation" in Allen, C. & Barr, W.J., eds., *Smart Cards* (New York, McGraw-Hill, 1997) 177.
52. Dow, S.L., "Airport Security, Terrorism, and the Fourth Amendment: A Look Back and a Step Forward" (1993) 58:4 J. of Air. L. 1149.
53. Drudmmond, R., "EDI and Internet" (1994) 4:2 EDI World 20.
54. Dubuc, C.E., "Air Travel, Tourism, Electronic Tickets and the Warsaw Convention in Cyberspace" (1997) 22:6 Air & Sp. L. 291.
55. Ducrest, J. "Legislative and Quasi-Legislative Functions of ICAO: Towards Improved Efficiency" (1995) XX:I Ann. Air & Sp. L. 343 at 354.
56. Effross, W.A., "Putting the Cards Before the Purse?: Distinctions, Differences, and Dilemmas in the Regulation of Stored Value Card Systems" (1997) 65 U.MKC L. Rev. 319.
57. Eser, G.O., "Impact of Automation on the Airline Business" (1986) 11 Ann. Air & Sp. L. 3.
58. Faller, E., "Aviation Security: The Role of ICAO in Safeguarding International Civil Aviation Against Acts of Unlawful Interference" (1992) XXVII:I Ann. Air & Sp. L. 369.
59. Feeley, M.J., "EU Internet Regulation Policy: The Rise of Self-Regulation" (1999) 22 B.C. Int'l & Comp. L. Rev. 159.
60. Feldman, D., "Privacy-related Rights and their Social Value", in P. Birks, ed., *Privacy and Loyalty* (Oxford: Clarndon Press, 1997).
61. Fenrich, W.J., "Common Law Protection of Individual's Rights in Personal Information" (1996) 65 Fordham L. Rev. 951.
62. Field, R.L., "The Electronic Future of Cash: Survey: 1996: Survey of the Year's Developments in Electronic Cash Law and The Laws Affecting Electronic Banking in the United States" 46 Am. U.L. Rev. 967.
63. Fiorita, D.M., "Aviation Security: Have All the Questions Been Answered?" (1995) XX:II Ann. Air & Sp. L. 69.
64. Fiorita, D.M., "The Warsaw Convention and Electronic Ticketing: Neither Ticketless nor Paperless" (1997) XXII Ann. Air & Sp. L.159
65. FitzGerald, G.F., "Unlawful Interference with Civil Aviation" in A. Kean, ed., *Essays in Air Law* (Netherlands: Martinus Nijhoff, 1982).

66. Flaherty, D.H., "Some Reflections on Privacy and Technology" (1999) 26 Man. L.J. 219.
67. Flaherty, D.H., "On the Utility of Constitutional Rights to Privacy and Data Protection" (1991) 41 Case W. Res. 831.
68. Foschio, L.G., "Motor Vehicle Records: Balancing Individual Privacy and the Public's Legitimate Need to Know" in T.R. Kuferman, ed., *Privacy and Publicity* (London: Meckler, 1990).
69. Freese, J., "Seven Years of Swedish Data Legislation - Analysis of Impact and Trend for the Future" in *Informatique et Protection de la Personnalité* (Saint-Paul Fribourg: Editions Universitaires Fribourg Suisse, 1981).
70. Freund, P.A., "Privacy: One Concept or Many" in J.R. Pennnock & J.W. Chapman, eds., *Privacy* (New York: Atherton Press, 1971).
71. Fried, C., "Privacy: Economics and Ethics A Comment on Posner" (1978) 12 Ga. L.Rev. 423.
72. Fromholz, J.M., "The European Union Data Privacy Directive" (2000) 15 Berkeley Tech. L. J. 461.
73. Gale, S., "The Impact of Information Technology Upon Civil Practice and Procedure" in L. Edwards & C. Waelde, eds., *Law & the Internet* (Oxford: Hart Publishing, 1997).
74. Gavison, R., "Privacy and the Limits of the Law" (1980) 89 Yale L.J. 421.
75. Gellman, R.M., "Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules" (1996) 41 Vill. L. Rev. 129.
76. Gellman, R.M., "Fragment, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions" (1993) 6 Software L.J. 199.
77. Glenn, H.P., "The Right to Privacy in Quebec Law" in D. Gibson, ed., *Aspects of Privacy Law* (Toronto: Butterworths, 1980).
78. Haanappel, P.P.C., "The IATA Conditions of Contract and Carriage for Passengers and Baggage" (1974) 9 Eur. Transp. L. 650.
79. Heydrich, M.W., "A Brave New World: Complying with the European Union Directive on Personal Privacy Through the Power of Contract" (1999) 25 Brooklyn J. Int'L L. 407.
80. Humphreys, B., "Computer reservation systems" in J. Pavaux, ed., *Air Transport: Horizon 2020* (Paris: Institut du Transport Aérien, 1995).
81. I.H. Ph. Dideriks-Verschoor, "Automation and Air Law" (1987) XII Ann. Air & Sp. L. 15.
82. Jueneman, R.R. & Robertson, Jr., R.L., "Biometrics and Digital Signatures in Electronic Commerce" (1998) 38 Jurimetrics J. 427
83. Jurevic, A.M., "When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail" (1998) 66 Univ. of Missouri at Kansas City L. Rev. 809.
84. Kahn, A., "Airline Deregulation - A Mixed Bag, But a Clear Success Nevertheless" (1988) 16 Transp. L.J. 229.
85. Kang, J., "Information Privacy in Cyberspace Transaction" (1998) 50 Stan. L. Rev.1193.
86. Karafiol, E., "The Right to Privacy and the SIDIS Case" (1978) 12 Ga. L. R. 513.
87. Keenan, W., Rea, M. & Hubbard, G., "Components of the Business Proposition" in C. Allen & W.J. Barr, eds., *Smart Cards* (New York: McGraw-Hill, 1997).

88. Kaufman Winn, J., "Clash of the Titans: Regulating the Competition between Established and Emerging Electronic Payment Systems" (1999) 14 Berkeley Tech. L.J. 675.
89. Killerlane, III, J.J., "Finger Imaging: A 21st Century Solution to Welfare Fraud at our Fingertips" (1995) Fordham Urb. L.J. 1327.
90. Kirby, J.M., "Legal Aspects of Transborder Data Flows" (1991) 9 Computer L.J. 233.
91. Kotch, K.J., "Addressing the Legal Problems of International Electronic Data Interchange: The Use of Computer Records as Evidence in Different Legal Systems" (1992) 6 Temple Int'l & Comp. L.J. 451.
92. Kraus, J.L., "On the Regulation of Personal Data Flows in Europe and the United States" (1993) Colum. Bus. L. Rev. 59, citing Justice M. Kriaby, "Legal Aspects of Transborder Data Flows" (1991) 11 Computer L.J. 233.
93. Laperrière, R., "The Quebec Model of Data Protection: A Compromise between *Laissez-Faire* and Public Control in a Technological Era" in Bennett, C.J. & Grant, R., eds., *Visions of Privacy - Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999).
94. Lloyd, I.J., "Data Protection" in C. Redd, ed., *Computer Law* (London: Blackstone Press Limited, 1996) 325.
95. Lyck, P. & Dormic, B.A., "Electronic Ticketing under the Warsaw Convention: The Risk of 'Going Ticketless' on International Flights" (1997) 22:1 Air & Sp. L.13.
96. Lyon, D. & Zureik, E., "Surveillance, Privacy, and the New Technology" in D. Lyon & E. Zureik, eds., *Computers, Surveillance, and Privacy*, (Minneapolis: University of Minnesota Press, 1996).
97. Malotky, L.O., "Advance Technologies Are Beginning to Have and Impact on the Quality and Cost of Aviation Security" (1995) 50:10 ICAO J. 9.
98. Manning, S., "The United States' Response to International Air Safety" (1195-1996) 61 J. of Air L. 505 at 511.
99. Margo, R.D., "Legal Aspect of Electronic Ticketing" (1997) XXII Ann. Air & Sp. L. 177.
100. Martin, C., "Mailing List, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem" (1998) 35 Hous. L. Rev. 801.
101. Martin, P., "Phone in, Turn up, Take-off, A Look at the Legal Implications of Self-service Ticketing" (1995) 20:1 Air & Sp. L. 189.
102. Martin, P., "Ticketless (but not documentless) travel" (1995) 14:6 Lloyd's Aviation L. 1.
103. Mayer-Schonberger, V., "Trans-Atlantic Information Privacy Legislation and Rational Choice Theory" (1999) 67 George Wash. L. Rev. 1309
104. Matthews, M.E., "Credit Cards - Authorised and Unauthorised Use" (1994) 13 Ann. Rev. Banking L. 233.
105. McAdams, R., "The Origin, Development, and Regulation of Norms" (1997) 96 Mich. L. Rev. 425.
106. McCallen, A., "Non-Immigration Visa Fraud: Proposals to End the Misuse of the L Visa by Transnational Criminal Organisations as a Method of Illegal Immigration" (1999) 32 Vand. J. Transnat'l L. 237.
107. McKeon, Jr., R.W., "Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena" (1994) 12 J. Marshal J. Computer & Info. L. 511
108. McMunn, M., "Aviation Security and Facilitation Programmes are Distinct but Closely Intertwined" (1996) 51:9 ICAO J. 7.

109. Mell, P., "A Hitchhiker's Guide To Trans-Border Data Exchanges Between EU Member States and the United States under the European Union Directive on the Protection of Personal Information" (1991) 9 Pace Int'l L. Rev. 147.
110. Milde, M., "The Chicago Convention - Are Major Amendments Necessary or Desirable 50 Year Later?" (1994) XIX:I Ann. Air & Sp. L. 401.
111. Milde, M., "The Role of ICAO in the Suppression of Drug Abuse and Illicit Trafficking" (1988) XIII Ann. Air & Sp. L. 133.
112. Milde, M., "Interception of Civil Aircraft vs. Misuse of Civil Aviation" (1986) XI Ann. Air & Sp. L. 105.
113. Milde, M., "The International Fight Against Terrorism in the Air" in J. Cheng, ed., *The Use of Airspace and Outer Space for all Mankind in the 21st Century* (Netherlands: Kluwer International, 1995) 141.
114. Mirmina, S.A., "Aviation Safety and Security - Legal Developments" (1998) 63 J. of Air L. 547.
115. Monahan, P.A., "Deconstructing Information Walls: The Impact of the European Data Directive on U.S. Businesses" (1998) 29 Law & Pol'y Int'l Bus. 275.
116. Mroz, D.M., "Credit or Debit? Unauthorised Use and Consumer Liability Under Federal Consumer Protection Legislation" (1999) 19 N. Ill. U. L. Rev. 589.
117. Murphy, R.S., "Property Rights in Personal Information: An Economic Defence of Privacy" (1996) 84 Geo.L.J.2381.
118. Myers, J.M., "Creating Data Protection Legislation in the United States: An Examination of Current Legislation in the European Union, Spain and the United States" (1997) 29 Case W. Res. J. Int'l L. 109.
119. O'Connor, S.M., "The de Minimis Exemption of Stored Value Cards From Regulation E: An Invitation to Fraud?" (1998) 5 Rich. J.L. & Tech. 6.
120. O'Keefe, C., "Immigration Issues and Airlines: An Update" (1997) 63:1 J. of Air L. 17.
121. Pearce, G. & Platten, N., "Achieving Personal Protection in the European Union" (1998) 36 J. Common Mkt. Stud. 529.
122. Pearce, G. & Platten, N., "Orchestrating Transatlantic Approaches to Personal Data Protection: A European Perspective" (1999) 22 Fordham Int'l L. J. 2024.
123. Piera, A., "La Tarjeta de Crédito" (1998) 8 Revista Juridica U. Católica de Asunción 69.
124. Pooley, J.H.A. & Shaw, D.M., "The Emerging Law of Computer Networks: Finding out what's there: technical and legal aspect of discovery" (1995) 4 Intell. Prop. L.J. 57.
125. Posner, R., "The Right of Privacy" (1978) 12:3 Ga. L. Rev. 393.
126. Poullet, Y., "Data Protection between Property and Liberties" in H.W.K. Kaspersen & A. Oskamp, eds., *Amongst Friends in Computers and Law - A Collection of Essays in Remembrance of Guy Vandenberghe* (Deventer, The Netherlands: Kluwer Law and Taxation Publishers, 1990).
127. Prosser, W.L., "Privacy" (1960) 48:3 Cal. L. Rev. 383.
128. Provenza, K., "Identity Theft: Prevention and Liability" (1999) 3 N.C. Banking Inst. 319.
129. Prowda, J.B., "A Layer's Ramble Down the Information Superhighway: Privacy and Security of Data" (1995) 64 Fordham L. Rev. 738.
130. Ratha, N.K. & Bolle, K., "Smart Card Based Authentication" in A. Jain, R. Bolle & S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (Boston: Kluwer Academic Publishers, 1999)

131. Reed, C., "EDI: Contractual and Liability Issues" (1989) 6 Computer L. 36; J.A. Smith, "Are Your EDI Transactions Safe? (A risk assessment methodology for EDI unclassified/sensitive information)" (1994) 5 CALS J. 76.
132. Reidenberg, J.R., "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" (1992) 44 Fed. Com. L. J. 195.
133. Reidenberg, J.R., "Restoring Americans' Privacy in Electronic Commerce" (1999) 14 Berkely Tech. L.J. 771.
134. Reidenberg, J.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. 497.
135. Reser, H.E., "Airline Terrorism: the Effect of Tightened Security on the Right to Travel" (1998) 63:4 J. of Air L. 819.
136. Ritter, J.B., "Current Issues in Electronic Data Interchange: Defining International Electronic Commerce" (1992) 13 J. Int'l L. Bus. 3.
137. Roch, M.P., "Filling the Void of Data Protection in the United States: Following the European Example" (1996) 12 Computer & High Tech. L.J. 71.
138. Rose, P., "A Market Response to the European Union Directive on Privacy" (1999) 4 UCLA J. Int'l L. & For. Aff. 445.
139. Rosler, D.B., "The European Union's Proposed Directive for the Legal Protection of Databases: A New Threat to the Free Flow of Information" (1995) 10 High Tech. L.J. 105
140. Sabett, R.V., "International Harmonisation in Electronic Commerce and Electronic Data Interchange: A Proposed First Step Towards Signing in the Digital Dotted Line" (1998) 46 Am. L.R. 511.
141. Samuelson, P., "A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy", Book Review of *Data Privacy Law, Study of United States Data Protection* by P.M Schwartz & J.R. Reidemberg (1999) 87 Cal. L. Rev. 751.
142. Schwartz, P.M., "Privacy and the Economics of Personal Health Care Information" (1997) 76 Tex. L. Rev. 1
143. Schwartz, P.M., "European Data Protection Law and Restrictions on International Data Flows" (1995) 80 Iowa L. Rev. 471.
144. Shafter, G., "Globalisation and Social Protection: The Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards" (2000) 25 Yale J. Int'l L. 1.
145. Sherwood, J., "EDI Security" in B. Welch, ed., *Electronic Banking and Security*, (Cambridge, Massachusetts: Blackwell Publishers, 1994).
146. Shorr, S., "Personal Information Contracts: How To Protect Privacy Without Violating the First Amendment" (1995) 80 Cornell L. Rev. 1756.
147. Simitis, S., "From the Market to the Polis: The EC Directive on the protection for Personal Data" (1995) 80 Iowa L. Rev. 445.
148. Smith, B.W. & Wilson, R.J., "How Best to Guide the Evolution of Electronic Currency Law" (1997) 46 Am. U.L. Rev. 1105.
149. Simons, M.S., "A Review of Issues Concerned with Aerial Hijacking and Terrorism: Implications for Australia's Security and the Sydney 2000 Olympics" (1998) 63:4 J. of Air L. 731.
150. Sovern, J., "Opting In, Opting Out, or No Options at All: The Fight For Control of Personal Information" (1999) 74 Wash. L. Rev. 1033.

151. Stankey, R.F., "Internet Payment Systems: Legal Issues Facing Businesses, Consumers and Payment Service Providers" (1999) 6 CommLaw Conspectus 11.
152. Sterre, R.S., "Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act" (1998) 33 Val. U. L. Rev. 231.
153. Sundberg, J., "Legitimate Responses to Aerial Intruders" (1985) X Ann. Air & Sp. L. 251.
154. Szwak, D.A., "Credit Cards in America" (1995) 13 J. Marshall J. Computer & Info. L. 573.
155. Tan, D.R., "Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union" (1999) 21 Loy. L.A. Int'l & Comp. L.J. 661.
156. Thaker, J.S., "Model Clause on Aviation Security for Bilateral Air Transport Agreements" (1992) XXVII:II Ann. Air & Sp. L 403.
157. Tompkins, Jr., G.N., "Enforcement of Aviation Safety Standards" (1995) XX:I Ann. Air & Sp. L 319.
158. Trubow, G.B., "The European Harmonisation of Data Protection Laws Threatens US Participation in Trans Border Data Flow" (1992) J. Int'l. Bus. 159.
159. van Arkel, J. & van der Tuin, A., "Who Did You Say You Were" in Knopjes, F. & Lakerman, P.J., eds., *Chip Card: Trump Card?* (Netherlands: National Criminal Intelligence Division, 1999).
160. van Dam, R.D., "Recent Developments in Aviation Safety Oversight" (1995) XX:I Ann. Air & Sp. L. 307.
161. Warren, S.D. & Brandeis, L.D., "The Right of Privacy" (1890) 4:5 Harv. L. Rev. 193.
162. Wilson, C.L., "Extending Bank Regulation to Electronic Money and Beyond" (1997) 30 Creighton L. Rev. 671.
163. Woodward, Jr., "Biometric Scanning, Law & Policy: Identifying the Concerns-Drafting the Biometric Blueprint" (1997) 59 U. Pitt. L. Rev. 97.
164. Woodward, Jr., Biometrics; Identifying Law & Policy Concerns" in A. Jain, R. Bolle & S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society* (Boston: Kluwer Academic Publishers, 1999).
165. Wounters, W., "The Hybrid Relationship Between Computer Reservation Systems (CRSs) and Airlines" (1997) Aviation Q. 346.
166. Yost, E.G., "Immigration and Nationality Law" (1997) 31 Int'l Lawyer. 589
167. Zagaris, B. & MacDonald, S.B., "Money Laundering, Financial Fraud, and Technology: The Perils of an Instantaneous Economy" (1992) 26 GW J. Int'l L. & Econ. 62.
168. Zimmerman, J.A., "Transborder Data Flow: Problems with the Council of Europe Convention, or Protecting States from Protectionism" (1982) 4 J. Intl. L. Bus. 601.

Magazine Articles

(in alphabetical order)

1. Airline Industry Information, "AII Provides a Roundup of News not Reported Elsewhere" (September 1997).
2. Airline Industry Information, "Ticket Sold Online to Be Less Flexible than Those Paid for Through Travel Agents/Direct Under New Rules" (November 1999).
3. Airline Industry Information, "US Travel Agents complain of internet sales" (October, 1997).
4. Airline Industry Information, "Travel agents being hit by growing e-ticketing popularity" (July 1999)
5. Airline Industry Information, "US Airways expands electronic ticketing to Canada" (October 1997).
6. Airline Industry Information, "IBM works with IATA to improve electronic ticketing" (August, 1999).
7. Airline Industry Information, "Asian Economic Problems are hampering e-commerce uptake in aviation industry" (May 1999).
8. Airline Industry Information, "Electronic sales overtake paper sale at United Airlines" (June 1999).
9. Airline Industry Information, "NW introduces E-ticketing for US/Canada to Asia routes" (July 1999).
10. Airline Industry Information, "Electronic ticketing becoming more and more popular" (July 1999)
11. Airline Industry Information, "America West, Continental introduce interline e-ticketing" (October 1999).
12. Airline Industry Information, "JAL to Offer E-ticketing service" (April 2000).
13. Airline Industry Information, "Chinese-Taiwanese ticketing agreement arranged" (July 1997).
14. Airline Industry Information, "Airlines eager to promote online ticket sales" (October 1998).
15. Airline Industry Information, "Unisys introduces new ticketing product" (July 1997).
16. Airline Industry Information, "Airlines on the internet" (January 1997).
17. Airlines International, "IBM Providing Travel Solutions in a fast changing world" (January 1997).
18. Airlines International, "The crazy huge thing called the Internet" (January 1997).
19. Airlines International, "Getting a Grip on the Internet" (January 1997)
20. Airlines International, "Insight on IATA" 4:5 (September 1998) 54.
21. Airports, "Continental Begins Self-Ticketing Service at Airports" (April 1995).
22. Airports, "United Now Offering Electronic Ticketing Nationwide" (September 1995).
23. Airports, "United to offer electronic ticketing on international flights" (November 1995).
31. Airport World, "Beating ICAO Passenger Processing Times" 3:3 (June-July 1998).
24. Aviation Week & Space Technology, "Online ticket sales soaring at Southwest" (March 2000).
25. Baker, C., "British Airways moves towards internet network" *Airline Business* (February 2000).

26. BCBR.com, "Tips for travel with electronic airline ticketing" online: http://www.bcbr.com/aug96/eside2.html (date accessed: 17 May 2000).
27. Blank, D., "Raising the Internet Stakes" *Airline Business* (September 1999).
28. Bond R., & Guillebeaud, D., "Surviving the Customer" *Airline Business* (March 1997) 54.
29. Borgo, B. & Bull-Larsen, B., "Losses: What Losses?" *Airline Business* (August 1998) 54.
30. Bray, R., "Immigration Taking Smart Steps" *Financial Times* XI (4 September 1997).
31. Canada Newswire, "Air Canada introduces electronic ticketing to Bermuda" (February 1999).
32. Canada Newswire, "Air Canada Expands Electronic Ticketing Throughout North America" (November 1998).
33. Conway, P., "Cargo on-line" *Airline Business* (February 2000) 76.
34. De Pommes, C., "Are you IT-Compatible?" *Airline Business* (July 1998) 26.
35. Feldman, J.M., "Cyberspace Direct" *Air Transport World* (August 1996).
36. Feldman, J.M., "E-commerce: The future is now" *Air Transport World* (November 1999).
41. Fenner, S., "Playing Smart Card" *Airline Business* (October 1998) 83.
37. Flint, P., "Bigger than the Internet?" *Air Transport World* (September 1998) 54.
38. Flint, P., "Cyber hope or cyber hype?" *Air Transport World* (October 1996) 25.
39. Gallacher, J., "Playing Your Cards Right" *Airline Business* 15:8 (August 1999) 46.
40. Gallacher, J., "Phone Alone" *Airline Business* (May 1999) 43.
41. Gallacher, J., "Easy does it" *Airline Business* (December 1997) 61.
42. Gallacher, J., "Holding the pieces together" *Airline Business* (January 1998) 28.
43. Gallacher, J., "Cargo chasing the value chain" *Airline Business* (November 1998) 52
44. Gill, T., "Sabre" *Airline Business* (January 2000).
45. Gormley, M., "Aviation on the Internet" *Business & Commercial Aviation* (September 1995) 76.
46. Harrop, P., "Playing the Smartcard" *Air Transport World* 14:10 (October 1998) 81.
47. Hawes, M., "For Growth You Need Vision" *Airlines International* 5:1 (January 1999) 28.
48. Heitmeyer, R., "Biometric ID and Airport Facilitation" *Airport World* 5:1 (March 2000) 18.
49. Jirasakunthai, C., "Qantas-BA to launch e-ticketing" *Nation* (May 1999).
50. Jones, L., "Skating on thin ice" *Airline Business* (February 1997) 36.
51. Judge, J., "No free ride for automatic ticketing" *Aviation Informatics* (April 1994).
52. Levere, J., "On-Line, A new web challenger" *Airline Business* (November 1998) 49.
53. Levere, J., "Agents of Change" *Airline Business* (August 1997) 52.
54. Levere, J., "Netting a bargain" *Airline Business* (August 1999) 18.
55. Levere, J., "No Ticket to ride catching on fast" *Airline Business* (September 1997) 122.
56. Levere, J., "The Smart Airlines Take Credit Cards" *Airline Business* (March 1998) 79.
57. Levere, J., "Low Fares capture more web sales" *Airline Business* (January 1998) 62.
58. Levere, J., "Internet pursuit heats up" *Airline Business* (December 1998).
59. Levere, J., "Alaska offers internet check-in" *Airline Business* (April 2000).
60. Levere, J., "Paperless Journey - Electronic Ticketing" *Airline Business* (January 1995).

61. M2 Press wire, "Electronic ticketing now available on Air Canada's Caribbean routes" (July 1999).
62. M2 Press wire, "Cathay Pacific launches electronic ticketing" (January 1998).
63. M2 Press wire, "Delta Air Lines introduces electronic ticketing to and from Latin America" (April 1999).
64. M2 Press wire, "United Airlines and Air Canada Introduce Airline Industry's First Inter-Airline Electronic Ticketing" (June 2000).
65. M2 Press wire, "American & United Airlines to develop interline electronic ticketing product" (May 1998).
66. Magnay, K., "Creative Passenger Processing Options on Show" *Aviation Informatics* (November 1996) 21.
67. Momberger, M., "Speeding Up Air Travel on the Ground" *Airport Forum* XXV:3 (June 1995).
68. Musselwhite, J., "Air Cargo Information Systems" *Aviation Informatics* (October 1995) 4.
69. Nicol, J., "Passports for Sale" *Maclean's* (3 April 2000) 16.
70. Odell, M., "Freight Frighteners" *Airline Business* (March 1997) 60.
71. Osborn, K., "Spinning a Web" *Airline Business* (January 2000).
72. O'Toole, K., "Gaining an edge" *Airline Business* (November 1998) 70.
73. O'Toole, K., "Getting the e-price right" *Airline Business* (December 1999).
74. O'Toole, K., "Up to the minute" *Airline Business* (December 1999).
75. O'Toole, K., "IT trends Survey" *Airline Business* (August 1999).
76. Ott, J., "Airlines Using Web for More than E-ticketing" (March 2000).
77. Phillipson, F., "Wheeling out the service" *Airline Business* (January 1997) 40.
78. Philipson, F., "Yields making cargo pay" *Airline Business* (November 1998) 64.
79. PR Newswire, "United Airlines' E-Ticket (SM) Service lands in Chile and Venezuela" (June 1999).
80. PR Newswire, "Delta air Lines Introduces Electronic Ticketing with Delta Connection Carriers" (April 1999).
81. PR Newswire, "Corporate travel decision-makers endorse electronic ticketing for air travel" (February 1996).
82. Russel-Wailling, E., "The Ticketless transition" *Airport World* (July 1997).
83. Schwartz, N. & Zea, N. "Surfing the value" *Airline Business* (July 1999) 68.
84. Seward, D. "Airbus Announces 555-Seat Plane" *Associated Press* (23 June 2000) online: http://biz.yahoo.com/apf/000623/france_air_7html (date accessed: 23 June 2000).
85. Stillwell, J., "Will Smart Cards Take Flight?" *Aviation Informatics* (November 1996) 25.
86. Tompkins, P., "Immigration Controls at International Airports in the 21st Century" *Aviation Security International* 3:6 (March 1994).
87. Transport Europe, "Intermodality: Forward Towards an Integrated European System" 58 (19 January 1996).
88. Velocci, A., "Southwest to tap internet for ticketless travellers" *Aviation Week & Space Technology* (June 1995).
89. Vis, B., "The Importance of Smart Cards" *Airport World* 3 (15 June 1996) 25.
90. Walker, K., "The King of low-cost" *Airline Business* (June 1999) 38.
91. Walker, K., "Proceed with care" *Airline Business* (June 1997) 70.
92. Walters, B., "Airport go-faster strips" *Jane's Airport Review* (October 1994).
93. Whitaker, R., "Airline Revolution Gathers Pace" *Airline Business* (August 1998) 7.

94. Whitaker, R., "Channel your sales energies" *Airline Business* (April 1998).

Internet Sources

(in alphabetical order)

1. Airbus Industrie, News Release "A3XX Receives Authorisation to Offer" (23 June 200); "ILFC Interested in the A3XX" (7 June 2000) online: http://www.airbus.com/media/press.asp (date accessed: 23 June 2000).
2. Airbus Industrie, "A3XX Economics" online: http://www.airbus.com/products/A3XX_economics.html (date accessed: 20 June 2000).
3. Airbus Industrie, "A3XX Commonality" online: http://www.airbus.com/producs/A3XX_commonality.html (date accessed: 20 June 2000).
4. Biometric Consortium, "Government Applications and Operations" online: http://www.biometrics.org/REPORTS/CTSTG96 (date accessed: 19 August 2000).
5. Boeing, "707 Family" online: http://www.boeing.com/commercial/707family/index.html (date accessed: 20 June 2000).
6. Boeing, "747-400 Family" online: http://boeing.com/commercial/747-400/family/index.html (date accessed: 20 June 2000).
7. Boeing, "747-400 Specifications" online: http://boeing.com/commercial/747-400/product.html (date accessed: 20 June 2000).
8. Boeing, "Worldwide Airplane Deliveries" online: http://www.boeing.com/commercial/cmo/4wa01.html (date accessed: 20 June 2000).
9. Boeing, "Current Market Outlook, Executive overview" online: http://www.boeing.com/commercial/cmo/1eo01.html (date accessed: 20 June 2000).
10. Boeing, "Current Market Outlook, Results by Region of the World" online: http://www.boeing.com/commercial/cmo/5apc1.html (date accessed: 20 June 2000).
11. Canada Customs and Revenue Agency, "CANPASS - Airport Extending Border Services" online: http://www.ccra-adrc.gc.ca/E/pub/cp/rc4062ed/rc4062ed.html (date accessed: 15 August 2000).
12. Canada Customs Revenue Agency, " Guidelines and General Information" online: http://www.ccra-adrc.gc.ca/E/pub/cm/d259/d259ed.html (date accessed: 15 August 2000).
13. Canadian Standards Association, "Model Code for the Protection of Personal Information" online: http://www.csa-international.org/english/product_services/ps_privacy.html (date accessed: 30 July 2000).
14. CNN, "Smart Cards: The Hassle-free Future of Travel?" online: http://cnn.com/tech/computing/9903/26/t_t/e.travel (date accessed: 23 June 2000).
15. Direct Marketing Association, "Privacy Promise Member Compliance Guide - Keeping Our Privacy Promise to Consumers" online: http://www.the-dma.org/library/privacy/privacypromise.shtml (date accessed: 13 July 2000).

16. Hays, R., "INS Passenger Accelerated Service System (INSPASS)" *Biometric Consortium* online: http://www.biometrics.or/epots/inspass.html (date accessed: 26 June 2000).
17. IATA, *World Air Transport Statistics* (Montreal: IATA, 2000). See also IATA, News Release PS/12/00 "2000 W.A.T.S. - More Passengers, Less Profits" (19 June 2000) online: http://www.iata.org/pr/pr00jung.html (date accessed: 20 June 2000).
18. IATA, News Release No. 13 "Customer Service, Liberalisation, and E-Commerce at Top of Airlines' Agenda" (6 June 2000) online: http://www.iata.org/pr/pr00junc.html (date accessed: 20 June 2000).
19. IATA, "Cargo Facilitation" online: Http://www.iata.org/cargo/facilitation.html (date accessed: 30 June 2000).
20. IATA, "IATA and Cargo EDI" Online: Http://www.iata.org/cargo/edi.html (date accessed 17 May 2000).
21. IATA, "Smart Card Technology" online; http://www.iata.org/smartcard/news.html (date accessed: 23 June 2000).
22. IATA, "Airline Industry Smart Card Developments" online: http://www.iata.org/smartcard/smartcard.html (date accessed: 23 June 2000).
23. IATA, "IINET - IATA service for the Air Transport industry" online: Http://www.iata.org/iinet/index.html (date accessed: 17 May 2000).
24. IATA, "Electronic Ticketing, Airline Industry ET Developments" online: Http://www.iata.org/eticket/eticket.html (date accessed: 17 May 2000).
25. IATA, "Simplifying Passenger Travel" online: http://www.iata.org/smartcard/article1.html (date accessed: 24 June 2000).
26. IBM, "American Express Licenses Smart Card Multiple Application Framework to Leading Industry Players" online: http://houns54.clearlake.ibm.com/solutions/travel/trapub.nsf/detailcontacts/American_Express_licenses_smart_card_multiple_application_framework_to_leading_industry_players?opendocument&detail=1 (date accessed: 23 June 2000).
27. ICAO, "Facilitation, Advance Passenger Information" online: Http://www.icao.org/ico.en/atb/fal/api.html (date accessed: 22 June 2000).
28. International Court of Justice, News Release 99/36, "Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie" (1 July 1999), online: http://www.icj-cij.org/icjwww/idocket/iluk/iluk2frame.html (date accessed: 14 July 2000).
29. Jeanniot, P.J., "The Future of the Airline Industry" (Economist Global Airlines Conference, 16 May 2000), online: http://www.iata.org/pr/speech2.html (date accessed: 20 June 2000).
30. Metropolitan Transportation Commission, "Aviation Forecasts Show Air Passengers Double by 2020" online: http://biz.yahoo.com/prnews/000712/ca_future_html (date accessed: 13 July 2000).
31. NCP, "Open Infrastructure for Chipcard Application" online: Http://www.ncp.nu/oic/brochureuk.html (date accessed: 30 June 2000).
32. OECD, First Report on the OECD Growth Project, *Is there a New Economy?* (12 June 2000), online: http://www.oecd.org/subject/growth/new_eco.pdf (date accessed: 13 July 2000).
33. Population Register Centre, News Release "Finnish Citizen Card and Electronic Identification" (22 November 1999), online: Http://www.vaestorekisterikeskus.fi/tied9931e.html (date accessed: 3 July 2000).

34. Population Register Centre, "Population information System in Finland" online: http://www.vaestorekisterikeskus.fi./hsteng.html (date accessed: 3 July 2000).
35. Privacy Commissioner of Canada, "Backgrounder Privacy Provisions Highlights" online: http://strategis.ic.gc.ca/virtual_hosts/e-com/english/fastfacts/43d8.html (date accessed: 28 July 2000.
36. Privacy Commissioner of Canada, "Implementation Schedule" online: http://www.privcom.gc.ca/english/02_06_02a_e.html (date accessed: 29 July 2000).
37. United Nations Economic Commission for Europe, "UN/EDIFACT Draft Directory" online: http://www.unece.org/trade/untdid/texts/d100_d.html (date accessed: 21 June 2000).
38. US Customs, "Advance Passenger System" online: http://www.customs.gov/impoexpo/tools/archives/vol2n01/moujul.htm#top (date accessed: 23 June 2000).
39. US Customs, "U.S. Customs Service Goals for the Year 2000 - High Impact Agency Initiative" online: http://www.customs.gov/about/hi-impact.html (date accessed: 23 June 2000).
40. US Customs, Department of the Treasure, "Announcement of a General Program Test: Procedure for Transfer of Accompanied (International) In-transit Baggage" online: http://www.customs.gov/new/fed-reg/notices/914538.html (date accessed: 23 June 2000).
41. US Department of Justice Immigration and Naturalization Service, "INS Passenger Accelerated Service System" online: http://www.ins.usdoj.gov/graphics/publicaffairs/factsheets/passfs.html (date accessed: 26 June 2000).