Article 13
Entry and Clearance Regulations

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

Contents

1 Control of Air Transport

This article forms the basis of ICAO's facilitation programme. The Assembly, at its 37th Session (Montreal, September/October 2010) adopted Resolution A37-20 (Consolidated statement of continuing ICAO policies in the air transport field) Appendix D of which was on development and implantation of facilitation provisions. The Resolution stated:

> *Whereas* Annex 9 — Facilitation, was developed as a means of articulating the obligations of Contracting States under Articles 22, 23 and 24 of the Convention and standardizing procedures for meeting the legal requirements referred to in Articles 10, 13, 14, 29 and 35;
>
> *Whereas* implementation of the Standards and Recommended Practices in Annex 9 is essential to facilitate the clearance of aircraft, passengers and their baggage, cargo and mail and manage challenges in border controls and airport processes so as to maintain the efficiency of air transport operations;
>
> *Whereas* it is essential that Contracting States continue to pursue the objective of maximizing efficiency and security in such clearance operations;
>
> *Whereas* the Convention on the Rights of Persons with Disabilities and its Optional Protocol, that had been adopted in December 2006 by the United Nations General Assembly, entered into force on 3 May 2008;

R. Abeyratne, *Convention on International Civil Aviation*,
DOI 10.1007/978-3-319-00068-8_14,

Whereas the development of specifications for machine readable travel documents by the Organization has proved effective in the development of systems that expedite the movement of international passengers and crew members through clearance control at airports while enhancing immigration compliance programmes; and

Whereas the development of a set of standard signs to facilitate the efficient use of airport terminals by travellers and other users has proved effective and beneficial;

The Assembly:

1. *Urges* Contracting States to give special attention to increasing their efforts to implement Annex 9 Standards and Recommended Practices;

2. Requests the Council to ensure that Annex 9 — *Facilitation,* is current and addresses the contemporary requirements of Contracting States with respect to administration of border controls, cargo and passengers, the protection of passenger and crew health and the accessibility to air transport by persons with disabilities;

3. Requests the Council to ensure that the provisions of Annex 9 — *Facilitation,* and Annex 17 — *Security,* are compatible with and complementary to each other;

4. *Requests* the Council to ensure that its specifications and guidance material in Doc 9303, *Machine Readable Travel Documents,* remain up to date in the light of technological advances and to continue to explore technological solutions aimed at improving clearance procedures; and

5. *Requests* the Council to ensure that Doc 9636, *International Signs to Provide Guidance to Persons at Airports and Marine Terminals*, is current and responsive to the requirements of Contracting States[1]

On machine readable travel documents (particularly passports and visas) the Resolution's Appendix D goes on to say the following:

Whereas the passport is the basic official document that denotes a person's identity and citizenship and is intended to inform the State of transit or destination that the bearer can return to the State which issued the passport;

Whereas international confidence in the integrity of the passport is essential to the functioning of the international travel system;

Whereas the veracity and validity of machine readable travel documents (MRTDs) depends on the documentation used to establish identity, confirm citizenship or nationality and assess entitlement of the passport applicant (i.e. "breeder" documentation);

Whereas Member States of the United Nations have resolved, under the Global Counter-Terrorism Strategy adopted on 8 September 2006, to step up efforts and cooperation at every level, as appropriate, to improve the security of manufacturing and issuing identity and travel documents and to prevent and detect their alteration or fraudulent use;

Whereas Resolution 1373 adopted by the United Nations Security Council on 28 September 2001 decided that all States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents;

Whereas high-level cooperation among States is required in order to strengthen resistance to passport fraud, including the forgery or counterfeiting of passports, the use of forged or counterfeit passports, the use of valid passports by impostors, the use of expired or revoked passports, and the use of fraudulently obtained passports;

Whereas the use of stolen blank passports, by those attempting to enter a country under a false identity, is increasing worldwide; and

Whereas ICAO provides assistance to States in all matters related to MRTDs including project planning, implementation, education, training and system evaluation services, and

[1]ICAO Doc 9958, Assembly Resolutions in Force (as of October 2010) at III-9 to III-10.

has set up the Public Key Directory (PKD) to strengthen the security of biometrically-enhanced MRPs (ePassports);

The Assembly:

1. *Urges* Contracting States to intensify their efforts to safeguard the security and integrity of the breeder documentation;

2. *Urges* Contracting States to intensify their efforts to safeguard the security and integrity of their passports, to protect their passports against passport fraud, and to assist one another in these matters;

3. *Urges* those Contracting States that have not already done so, to issue machine readable passports in accordance with the specifications of Doc 9303, Part 1;

4. *Urge*s Contracting States to ensure that the expiration date of non-machine readable passports falls before 24 November 2015;

5. *Urges* those Contracting States requiring assistance in implementing MRTD standards and specifications to contact ICAO without delay;

6. *Requests t*he Council to take appropriate measures to establish guidance on breeder documentation;

7. *Requests* the Council to continue the work on enhancing the effectiveness of controls on passport fraud by implementing the related SARPs of Annex 9 and developing guidance material to assist Contracting States in maintaining the integrity and security of their passports and other travel documents;

8. *Urges* those States issuing ePassports to join the ICAO PKD; and all receiving States to verify the digital signatures associated with the passports; and

9. *Urges* those Contracting States that are not already doing so to provide routine and timely submissions of lost and stolen passport data to Interpol's Automated Search Facility/ Stolen and Lost Travel Document Database.

On national and international cooperation on facilitation matters the Resolution states:

Whereas there is a need for continuing action by Contracting States to improve the effectiveness and efficiency of clearance control formalities;

Whereas the establishment and active operation of national facilitation committees is a proven means of effecting needed improvements;

Whereas cooperation on facilitation matters amongst Contracting States and with the various national and international parties interested in facilitation matters has brought benefits to all concerned; and

Whereas such cooperation has become vital in the light of the proliferation of non-uniform passenger data exchange systems that adversely affect the viability of the air transport industry;

The Assembly:

1. *Urges* Contracting States to establish and utilize national facilitation committees and adopt policies of cooperation on a regional basis among neighbouring States;

2. *Urges* Contracting States to participate in regional and subregional facilitation programmes of other intergovernmental aviation organizations;

3. *Urges* Contracting States to take all necessary steps, through national facilitation committees or other appropriate means, for:

a) regularly calling the attention of all interested departments of their governments to the need for:

1) making the national regulations and practices conform to the provisions and intent of Annex 9; and

2) working out satisfactory solutions for day-to-day problems in the facilitation field; and

b) taking the initiative in any follow-up action required;

4. *Urges* Contracting States to encourage the study of facilitation problems by their national and other facilitation committees and to coordinate the findings of their committees on facilitation problems with those of other Contracting States with which they have air links;

5. *Urges* neighbouring and bordering States to consult one another about common problems that they may have in the facilitation field whenever it appears that these consultations may lead to a uniform solution of such problems;

6. *Urges* Contracting States to encourage their aircraft operators to continue to cooperate intensively with their governments as regards:

a) identification and solution of facilitation problems; and

b) developing cooperative arrangements for the prevention of illicit narcotics trafficking, illegal immigration and other threats to national interests;

7. *Urges* Contracting States to call upon international operators and their associations to participate to the extent possible in electronic data interchange systems in order to achieve maximum efficiency levels in the processing of passenger and cargo traffic at international terminals;

8. *Urges* Contracting States, in their use of electronic data interchange systems, to ensure that their passenger data requirements conform to international standards adopted by relevant United Nations agencies for this purpose; and

9. *Urges* States and operators, in cooperation with interested international organizations, to make all possible efforts to speed up the handling and clearance of air cargo, while ensuring the security of the international supply chain.

Illegality or irregularity in migratory movements, although generally viewed from the perspective of the destination country, may occur in either one of the countries of origin, transit or destination or all of them. The country of origin becomes involved when a person leaves that country without a valid passport or an equivalent document of identity as required by national legislation. As regards the country through which an illegal migrant travels—or the transit country, its laws may be infringed upon if the person being smuggled did not have a transit visa to travel through that country. From the perspective of the country of destination, the main characteristics of illegal or irregular migration are more readily discernible. They are:

- The arrival by a person in a country and attempt thereafter to enter without compliance with required formalities or without authorization required by law for admission or stay in that country; or
- The cessation by a person of meeting conditions to which that person's stay or activity is subject.

Human migration is a compelling social indicator of the future and is driven by economic and social factors. Economically motivated migration characteristically takes place between countries which show a marked disparity in labour market situations (typically when one country shows shortage of labour and the other shows a surplus of labour) and sharply different levels of income.

The magnitude of the problem naturally spawns opportunities for profit making which in turn have given rise to the multi billion dollar human smuggling industry. In 1995, the Economist recorded:

> Around the world, smuggling organizations ranging in size and degree of sophistication are smuggling tens of thousands of people from poorer to richer countries. In the process, they are earning at least $7 billion per year, with the potential for even greater future profits.

The risk element involved in the smuggling of humans is far less than the smuggling of narcotics and therefore some gangs of notoriety have reportedly abandoned the drug trade in favour of smuggling humans. Human smuggling, to be defined as such, has to be composed of two different kinds of activity: the exchange of money or other form of payment between the would-be illegal migrant and smuggler; and the arrangement by a "facilitator" of passage across an international border. The movement has to be voluntary and the passage from one border to another should be illegal.

Smuggling is a popular recourse and an easy "way out" to the illegal immigrant who faces huge distances to travel; difficulties imposed by States' anti-immigrant restrictions; and difficulties adjusting to life in the host country.

Ironically, the last reason—difficulty in adjusting to life in the host country—works to the advantage of the smuggler. The process of payment, which is the essential part of the transaction of smuggling, is not always concluded with the act of smuggling. It may extend well beyond that point. The form and method of payment often reach insidious proportions of exploitation where the smuggler may discourage payment at the outset, making the illegal migrant an easy victim to exploitation and abuse. In many cases, the person seeking to be smuggled into a country illegally welcomes such deferral of payment making the smugglers' business flourish through easier recruitment of candidates for illegal migration. This situation also strengthens the position of the smuggler to tighten his grip on the migrants and use their virtually indentured services for unlawful and criminal activities.

A 1995 study on smuggled women carried out in Belgium suggests that although most women were not required to pay the smuggler in advance, a high proportion of them had found themselves on arrival to be required to perform various services to the smuggling network. The Vienna-based International Centre for Migration Policy Development (ICMPD) has revealed that 15–30 % of those who illegally went into Western Europe for purposes of employment or residence, estimated in 1993 to be a figure of 250,000–300,000 persons, used the services of smugglers.

2 United Nations Initiatives

Concerned that the activities of criminal organizations that profit illicitly by smuggling human beings were becoming a threat to the world community and recognizing that international criminal groups often convince individuals to migrate illegally by various means for enormous profit, the United Nations, at its 48th General Assembly in December 1993, adopted Resolution 48/102 on the prevention of smuggling aliens. This Resolution makes mention of smuggling of illegal migrants as an activity that endangers the lives of those smuggled and imposes severe costs on the international community. The United Nations noted that

smuggling of aliens can involve criminal elements in many States and condemned the practice of smuggling aliens in violation of national and international law. Resolution 48/102, while urging States to adopt measures to frustrate the objectives and activities of smugglers of illegal migrants, identifies the International Civil Aviation Organization (ICAO) as one of the specialized agencies of the United Nations that could consider ways and means to enhance international co-operation to combat the smuggling of aliens. At the same meeting, the General Assembly of the United Nations adopted Resolution 48/103 on crime prevention and international justice which reaffirmed the importance of the United Nations crime prevention and criminal justice programme and the crucial role the Organization has to play in promoting international co-operation in crime prevention and criminal justice. Resolution 48/103, *inter alia*, invites governments to lend their full support to the United Nations crime prevention and criminal justice programme.

In a subsequent 1997 resolution the United Nations General Assembly, at its fifty-first session, *inter alia*, recognized that international criminal groups often convinced individuals to migrate illegally by various means for enormous profits and that socio-economic factors influenced the problem of the smuggling of aliens and also contributed to the complexity of current international migration. The Assembly requested States to cooperate bilaterally and on a multilateral basis to prevent the use of fraudulent documents and reaffirmed the need to fully observe international and national law in dealing with the smuggling of aliens, including the provision of humane treatment and strict observance of all human rights of migrants.

Following up on its early initiatives, the United Nations General Assembly, at its 53rd Session, held in December 1998, adopted Resolution 53/111 establishing an open-ended inter-governmental *ad hoc* committee for the purpose of elaborating a comprehensive international convention against transnational organized crime. This Resolution gave rise to United Nations Convention against Transnational Organized Crime (which was still in draft form at the time of writing). The purpose of the Convention is to promote co-operation to prevent and combat transnational organized crime more effectively.

The Convention, by Article 3, requires Contracting States to establish as criminal offences, when committed internationally, the act of agreeing with one or more persons to commit a serious crime for any purpose relating directly or indirectly to the obtaining of financial or other material benefit and conducted by a person with knowledge which is tantamount to participating in criminal activities of an organized criminal group.

The Convention also considers organizing, aiding, abetting, facilitating or counselling the Commission of serious crime involving an organized criminal group to be a criminal offence. The Convention attributes to any person who aids and abets a crime, knowledge, intent, aim and purpose to commit such crime as provided for in Article 3, which makes the conduct by a person who knowingly aids and abets a criminal or criminal organizations a crime. The provision does not impute liability to any person who aids and abets a crime if that person ought to have known that his conduct would aid and abet a crime. In other words, any person who commits a crime under the Convention should essentially have the knowledge that his conduct would facilitate, aid or abet a crime.

The Protocol which supplements the Convention (which was also in draft form at the time of writing) specifically addresses the smuggling of migrants by land, air and sea and records *in limine*, the concern of the States Parties to the Protocol that the smuggling of migrants may lead to the misuse of established procedures for immigration, including those for seeking asylum.

The Protocol defines the smuggling of migrants as follows:

> "Smuggling of migrants" shall mean the procurement of the illegal entry into or illegal residence of a person in [a] [any] State Party of which the person is not a national or a permanent resident in order to obtain directly or indirectly, a financial or other benefit.

The Protocol defines illegal entry as crossing of borders without complying with the necessary requirements for legal entry into the receiving State.

The purposes of the Protocol are to prevent, investigate and prosecute the smuggling of migrants, when involving an organized criminal group, as defined in the Convention and to promote international cooperation to meet these objectives. The Protocol excludes the prosecution of persons who are smuggled, thus exclusively applying only to those responsible, directly or indirectly, in carrying out the act of smuggling.

Article 4 of the Protocol requires States Parties to enact domestic legislation that would criminalize, *inter alia*, the act of producing a fraudulent travel or identity document. This would also mean that a person who aids and abets such an act would be deemed to be criminally liable under the Convention. Article 12 of the Protocol provides that State Parties shall adopt such measures as may be necessary, in accordance with available means, to ensure that travel or identity documents issued by them are of such quality that they cannot easily be misused and cannot readily be unlawfully altered, replicated, falsified or issued. The provision also calls for States Parties to ensure the integrity and security of travel or identity documents issued by or on behalf of the States Parties and to prevent their unlawful creation, issuance and use.

3 Work of ICAO

The International Civil Aviation Organization has been making sustained efforts at adopting technical specifications for machine readable travel documents which are aimed at making illegal migration more difficult and facilitating air transport. Specifications for the machine readable passport and visa are already published and Sri Lanka is one of the countries which produce machine readable passports and actively participates in ICAO meetings.

4 The Machine Readable Passport (MRP)

The machine readable passport (MRP) is a passport that has both a machine readable zone and a visual zone in the page that has descriptive details of the owner. The machine readable zone enables rapid machine clearance, quick verification and instantaneous recording of personal data. Besides these advantages, the

MRP also has decided security benefits, such as the possibility of matching very quickly the identity of the MRP owner against the identities of undesirable persons, whilst at the same time, offering strong safeguards against alteration, counterfeit or forgery. Another advantage of the MRP is the fact that the document obviates the need for the passenger to lodge embarkation or disembarkation cards, on the assumption that countries installing automatic reader equipment would accept the data on the passport as sufficient for their clearance purposes. Of course, the MRP had to offer safeguards equal to or better than those of conventional passports and satisfy those control requirements already set by conventional passports and other travel documents in use throughout the world. Also, since it was only natural that a certain number of States would not have wished to issue the MRP or adopt new procedures related thereto, it was expected that a machine readable system and conventional passport procedures would operate side by side for some time.

Although the MRP may be produced and used as a single and separate card, it has to take booklet-form since most States still insist on entrance visas, which have to be accommodated in the passport. The MRP's dimensions are smaller than those of most traditional passports, its overall dimensions being 88.75 mm $\times$ 125.75 mm. The page has two areas—with the visual-inspection zone on top of the page as the first area, and the machine-readable zone at the bottom, as the second area. The visual inspection zone contains the photograph and personal data of the owner. At the bottom—in the machine readable zone, are prescribed data elements printed in machine readable form in a prescribed sequence and position. When being used, the MRP is opened at the page containing the visual-inspection and machine-readable zones and placed face down on a glass surface in the reading machine, thus activating an electro optical-scanning mechanism. The mechanism illustrates the two machine readable lines and surrounding background using a light source. The whole process operates on a principle of "light absorption" where the mechanism in the reader uses an optical sensor to measure the presence or absence of light reflecting off the page. The cumulative efforts of this "imagery" process and a computer installed in the reader then produces on the screen of the reader, all the information that the inspecting officer requires, such as the passport number, date of expiry of the passport, name of the issuing State, passport-owner's name, nationality, sex, date of birth, and optionally, national ID number. The computer also interrogates simultaneously, a data base containing a list of persons considered undesirable by the State of entry and the results thereof are displayed on the screen momentarily, enabling the inspecting officer to decide whether the bearer of the passport can be admitted to the country. This process takes a mere 10 s, and adds a tremendous impetus to the facilitation efforts of ICAO.

ICAO recommends the use of the MRP by all States, even if meagre traffic flows may not justify the use of reading equipment. The first MRP was issued in the United States of America in 1981 and since then, well over thirty five million MRPs have been issued world-wide, while millions more are being issued every year in countries such as Canada, Australia, Germany. Technical specifications for MRP's were first published by ICAO in the First Edition of Doc 9303 in 1980, based on Standard 7501 of the International Organization for Standardization (ISO).

Developments in technology and modern exigencies of prolific air travel however, dictated that the specifications contained in Doc 9303 be improved. As the ICAO Panel on Passport Cards had been extinct with the publication of its Fifth Report in 1978, the International Organization for Standardization (ISO) took it upon itself to establish a working group to update the provisions of Doc 9303 so that the outcome of their deliberations would be published as a new ISO Standard. The care taken by the ISO working group led to considerable time being taken by the working group, compelling ICAO to establish a new group to succeed its Panel on Passport Cards, namely, the Technical Advisory Group on Machine Readable Passports (TAG/MRP) which met for the first time in 1986. ICAO thus regained its lead in developing MRP specifications and co-ordinating with other organizations the task of developing a single set of specifications for machine readable travel documents. On the strength of ICAO's new leading role, the Air Transport Committee of ICAO widened the scope of the terms of reference of ICAO to include the development of specifications for machine readable visas and to provide for the Group's membership to include participation by the authorities responsible for visas. Accordingly, the ISO Technical Committee, in the light of ICAO's new role in updating specifications in Doc 9303, adopted a proposal to withdraw ISO Standard 7501, so that there would not be confusion by the introduction of double standards or "overlapping" of specifications of ICAO and ISO.

ICAO's terms of reference in the development of specifications for MRPs stem from the Chicago Convention itself which provides for ICAO's adoption of international Standards and Recommended Practices dealing inter alia with customs and immigration procedures. It is interesting that passports apply to other modes of international travel as well, and the fact that ICAO has been singly designated to adopt specifications speaks for the uniqueness of its facilitation programme.

5 The Machine Readable Visa

With the terms of reference of ICAO having been expanded to cover the development of machine readable visas (MRV), the Technical Advisory Group changed its name to read as the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), and, in 1992 released specifications relating to a machine readable visa. Since the visa is inextricably linked to the passport, both the MRP and the MRV go side by side, and are not considered in isolation. As long as visas were required and needed to be attached to the passport, it was difficult to envisage the development of a Passport Card, and a booklet type passport was required for visual inspection. The MRV therefore is the main reason for the retention of the MRP concept in its present form. Since MRVs can be accommodated in any type of passport (whether machine-readable or conventional) the placement of an MRV in a conventional, non machine readable passport would make that passport machine readable, worldwide.

6 Official Travel Documents

The Technical Advisory Group on Machine Readable Travel Documents has also developed the Size 1 and Size 2 Official Travel Documents (TD-1) which are cards conforming with Specification 7810 of the International Standards Organization (ISO) and is designed to be read by machine similar to the machine readable passport and visa. The specifications stipulate standards for official documents of identity which can be used for travel purposes in terms of acceptance of a person by a receiving State. In the same year during which the official travel document specifications were released by ICAO—1996—the Organization released specifications for machine readability of the crew member certificate.

At its eleventh meeting held in September 1999, the Technical Advisory Group on Machine Readable Travel Documents reiterated its support for continued work to develop a set of indicative, probably short term, test methods that could emulate failure modes commonly found in travel documents. The Group also approved in principle that the future direction of the Group's work should include inter alia, the development of specifications for an electronic visa; an integrated automated border clearance system; a survey of user requirements and current applicability of machine readable travel documents; and specifications for a logical record format for use with optional capacity exPANsion technologies.

The United Nations is forging ahead with preventive measures against the smuggling of illegal migrants through an ongoing effort. The rapid development of information technology has placed in the hands of States such sophisticated security tools as the machine readable travel document. A noteworthy corollary to this trend is that airlines will now be required to exercise more vigilance in the future, particularly with the introduction of the excellent initiative of the International Air Transport Association (IATA) for Simplified Passenger Travel (SPT) which has now gained momentum. The SPT concept, which is calculated to be essentially a tool for facilitating air travel, uses a smart card which confirms a traveller's identity through trip related information and biometric data which is encoded. The check-in takes less than a minute with the SPT card. Reportedly, a number of airlines are already well into the process of developing smart card technology. This could only mean that such a process, when developed by some, would have a coercive effect on other airlines which are able to follow suit. Failure to follow such industry practices may have negative implications on an air carrier's security record and may result in uncalled for legal liability.

6.1 The ePassport

Over 104 States are currently producing and using ePassports and there are approximately four hundred million in circulation. This accounts for 33 % of all passports used globally. The additional feature that the ePassport carries in the conventional machine readable passport is a chip containing biometric and biographic

information which have to be validated accurately, efficiently and quickly while retaining the security and integrity of the information. Ideally, an ePassport should be issued in accordance with the technical specifications approved by ICAO. However, this does not happen in all cases of issuance of ePassports. This lapse could seriously compromise global security. The nuances of this threat are described and discussed in this article against their legal background.

At a Symposium on machine readable travel documents, biometrics and security standards held at ICAO on 10–12 October 2012, experts addressed ICAO machine readable travel documents (MRTD) standards and specifications, identity management best practices and related border security issues. Foremost among these discussions was the ePassport, which is defined by ICAO as a passport which has a contactless integrated circuit (IC) chip within which is stored data from the machine readable passport page, a biometric measure of the passport and a security object to protect the public key infrastructure (PKI) cryptographic technology, and which conforms to the specifications of Doc 9303 part 1.[2] The ICAO Facilitation Manual defines the ePassport as a machine readable passport that has a contactless integrated circuit embedded in it and the capability of being used for biometric identification of the machine readable passport holder in accordance with the Standards specified in the relevant part of ICAO document 9303 (Machine Readable Travel Documents).[3] ePassports are easily recognised by the international ePassport symbol on the front cover.[4]

6.2 Biometric Identification

It is important to note that the operative terms in the definition of the ePassport are "biometric identification" and "public key infrastructure (PKI) cryptographic technology". Biometric technology involves a measurable, physical characteristic or

[2]Machine Readable Travel Documents Part 1 Volume 2 ICAO Doc 9303 Sixth Edition: 2006, at Page II-3 at Paragraph 6.1, Definitions.

[3]See The Facilitation Manual, Doc 9957, ICAO: Montreal, First Edition 2011, Definitions at X. ICAO has been working on the development of passports since 1968. The Seventh Session of the ICAO Facilitation Division in 1968 recommended that a small panel of qualified experts including representatives of the passports and/or other border control authorities, be established: to determine the establishment of an appropriate document such as a passport card, a normal passport or an identity document with electronically or mechanically readable inscriptions that meet the requirements of document control; the best type of procedures, systems (electronic or mechanical) and equipment for use with the above documents that are within the resources and ability of Member States; the feasibility of standardizing the requisite control information and methods of providing this information through automated processes, provided that these processes would meet the requirements of security, speed of handling and economy of operation.

[4]http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0021.shtm.

personal behavioral trait used to recognize the identity, or verify[5] the claimed identity of a person. Biometric identification has been defined as

> a generic term used to describe automated means of recognizing a living person through the measurement of distinguishing physiological or behavioural traits.[6]

Biometrics target the distinguishing physiological or behavioral traits of the individual by measuring them and placing them in an automated repository such as machine encoded representations created by computer software algorithms that could make comparisons with the actual features. Physiological biometrics that have been found to successfully accommodate this scientific process are facial recognition, fingerprinting and iris-recognition which have been selected by ICAO as being the most appropriate. The biometric identification process is four-fold: firstly involving the capture or acquisition of the biometric sample; secondly extracting or converting the raw biometric sample obtained into an intermediate form; and thirdly creating templates of the intermediate data is converted into a template for storage; and finally the comparison stage where the information offered by the travel document with that which is stored in the reference template.

Biometric identification gets into gear each time an MRTD holder (traveler) enters or exists the territory[7] of a State and when the State verifies his identity against the images or templates created at the time his travel document was issued. This measure not only ensures that the holder of the document is the legitimate claimant to that document and to whom it was issued, but also enhances the efficacy of any advance passenger information (API)[8] system used by the State to pre-determine the arrivals to its territory. Furthermore, matching biometric data presented in the form of the traveler with the data contained in the template accurately ascertains as to whether the travel document has been tampered with or not. A three way check, which matches the traveler's biometrics with those stored in the template carried in the document and a central database, is an even more efficacious

[5]To "verify" means to perform a one-to-one match between proffered biometric data obtained from the holder of the travel document at the time of inquiry with the details of a biometric template created when the holder enrolled in the system.

[6]Machine Readable Travel Documents Part 1 Volume 2, Preamble (*supra* note 3) at Page II-3 at Paragraph 4.1.

[7]The Chicago Convention, Preamble (*supra* note 1), defines, in Article 2, "territory of a State" as the land areas and territorial waters adjacent to the State under the sovereignty, suzerainty, protection and mandate of such State.

[8]API involves exchange of data information between airlines and customs authorities, where an incoming passenger's essential details are notified electronically by the airline carrying that passenger prior to his arrival. The data for API would be stored in the passenger's machine readable passport, in its machine readable zone. This process enables customs authorities to process passengers quickly, thus ensuring a smoother and faster clearance at the customs barriers at airports. One of the drawbacks of this system, which generally works well and has proven to be effective, is that it is quite demanding in terms of the high level of accuracy required. One of the major advantages, on the other hand, is the potential carried by the API process in enhancing aviation security at airports and during flight. See Abeyratne (2002a).

way of determining the genuineness of a travel document. The final and most efficient biometric check is when a four way determine is effected, were the digitized photograph is visually matched (non electronically) with the three way check described above.[9] In this context, it is always recommended that the traveler's facial image (conventional photograph) should be incorporated in the travel document along with the biometric templates in order to ensure that his identity could be verified at locations where there is no direct access to a central database or where the biometric identification process has not entered into the legal process of that location.

6.3 Public Key Infrastructure (PKI) Cryptographic Technology

PKI Cryptographic technology uses a brand new technique known as quantum cryptography, designed to eliminate the terrifying vulnerabilities that arise in the way digitally stored data are exposed to fraudulent use. This new technique uses polarized photons instead of electronic signals to transmit information along cables. Photons are tiny particles of light that are so sensitive that when intercepted, they immediately become corrupted. This renders the message unintelligible and alerts both the sender and recipient to the fraudulent or spying attempt. The public key directory—designed and proposed to be used by customs and immigration authorities who check biometric details in an electronic passport, is based on cryptography—and is already a viable tool being actively considered by the aviation community as a fail-safe method for ensuring the accuracy and integrity of passport information.

In order to assure inspecting authorities (receiving States) that they would know when the authenticity and integrity of the biometric data stored in the MRTD, which they inspect, are compromised and tampered with, the Public Key Infrastructure (PKI) scheme was developed by the TAG/MRTD, which has been pioneering work on the MRTD for over a decade.[10] The scheme is not calculated to prescribe global implementation of public key encryption, but rather acts as a facilitator enabling States to make choices in areas such as active or passive authentication,

[9]Issuing States must ensure the accuracy of the biometric matching technology used and functions of the systems employed if the integrity of the conducted checks are to be maintained. They must also have realistic and efficient criteria regarding the number of travel documents checked per minute in a border control situation and follow a regular biometric identification approach such as facial recognition, fingerprint examination or iris identification system.

[10]ICAO's terms of reference in the development of specifications for machine readable passports stem from the Chicago Convention which provides for ICAO's adoption of international Standards and Recommended Practices dealing, *inter alia,* with customs and immigration procedures. Chicago Convention, Preamble (*supra* note 2), Article 37(j). It is interesting that, although passports apply to other modes of international travel as well, ICAO has been singly recognized as the appropriate body to adopt specifications for MRTDs. This alone speaks for the uniqueness of ICAO's facilitation programme. See Machine Readable Travel Documents, *ICAO Doc 9303/6* Sixth Edition 2006, 1-1 to 1-3.

anti-skimming and access control and automated border crossing, among other facilitative methods. The establishment of a public key directory, through means of public key cryptology and in a PKI environment, is consistent with ICAO's ultimate aim and vision for the application of biometric technology on the fundamental postulate that there must be a primary interoperable form of biometric technology for use at border control with facilities for verification, as well as by carriers and the issuers of documents. This initial premise is inevitably followed by the assumption that biometric technologies used by document issuers must have certain specifications, particularly for purposes of identification, verification and the creation of watch lists. It is also ICAO's vision that States, to the extent possible, are protected against changing infrastructure and changing suppliers, and that a technology, once put in place, must be operable or at least retrievable for a period of 10 years.

6.4 Features and Purpose of the ePassport

The story of the passport—the precursor of the ePassport—starts with the birth of an individual and his birth certificate, which records the event of birth and time and place thereof. The Civil Registry is able, with this document to primarily establish the identity of the person at birth and inform his country of his details for purposes of maintaining census and vital statistics. The passport, which uses this information, gives a person a name and nationality that is required for him to travel internationally. The passport is a basic document in the transport by air of persons. Its use therefore is of fundamental importance as a travel document, not only because it reflects the importance of the sovereignty of a State and the nationality of its citizens but also because it stands for the inviolability of relations between States that are linked through air transport.

The key consideration of an ePassport is *Global Interoperability*—the crucial need to specify a system for biometrics deployment that is universally interoperable. a Logical Data Structure (LDS) for ePassports required for global interoperability. It defines the specifications for the standardized organization of data recorded to a contactless integrated circuit capacity exPANsion technology of an MRP when selected by an issuing State or organization so that the data is accessible by receiving States. This requires the identification of all mandatory and optional Data Elements and a prescriptive ordering and/or grouping of Data Elements that must be followed to achieve global interoperability for reading of details (Data Elements) recorded in the capacity exPANsion technology optionally included on an MRP (ePassport). The other considerations are *Uniformity*—the need to minimize via specific standard setting, to the extent practical, the different solution variations that may potentially be deployed by member States; *Technical reliability*—the need to provide guidelines and parameters to ensure member States deploy technologies that have been proven to provide a high level of confidence from an identity confirmation viewpoint; and that States reading data encoded by other States can be sure that the data supplied to them is of sufficient quality and integrity

to enable accurate verification in their own systems; *Practicality*—the need to ensure that specifications can be operationalized and implemented by States without their having to introduce a plethora of disparate systems and equipment to ensure they meet all possible variations and interpretations of the standards; and *Durability*—the requirement that the systems introduced will last the maximum 10-year life of a travel document, and that future updates will be backward compatible.

The major components of a biometric system are: *Capture*—acquisition of a raw biometric sample; *Extract*—conversion of the raw biometric sample data to an intermediate form; *Create template*—conversion of the intermediate data into a template for storage; and *Compare*—comparison with the information in a stored reference template.

In terms of security and privacy of the stored data, both the issuing and any receiving States need to be satisfied that the data stored on the IC has not been altered since it was recorded at the time of issue of the document. In addition, the privacy laws or practice of the issuing State may require that the data cannot be accessed except by an authorized person or organization. Accordingly ICAO has developed specifications in Section IV regarding the application and usage of modern encryption techniques, particularly interoperable public key infrastructure (PKI) schemes, to be used by States with their machine readable travel documents as made in accordance with the specifications set out in Doc 9303. The intent is primarily to augment security through automated means of authentication of MRPs and their legitimate holders internationally. In addition, ways and means are recommended to implement international ePassport authentication and to provide a path to the use of ePassports to facilitate biometric or e-commerce applications.

Annex 9[11] to the Convention on International Civil Aviation (Facilitation of Air Transport), in Standard 3.7 requires ICAO member States to regularly update security features in new versions of their travel documents, to guard against their misuse and to facilitate detection of cases where such documents have been unlawfully altered, replicated or issued. Recommended Practice 3.9 suggests that member States incorporate biometric data in their machine readable passports, visas and other official travel documents, using one or more optional data storage technologies to supplement the machine readable zone, as specified in Doc 9303, Machine Readable Travel Documents. The required data stored on the integrated circuit chip is the same as that printed on the data page, that is, the data contained in the machine-readable zone plus the digitized photographic image. Fingerprint image(s) and/or iris image(s) are optional biometrics for member States wishing to supplement the facial image with another biometric in the passport. Member States incorporating biometric data in their Machine Readable Passports are to store the data in a contactless integrated circuit chip complying with ISO/IEC 14443 and programmed according to the Logical Data Structure as specified by ICAO.

[11]Annex 9 to the Convention on International Civil Aviation, 12th Edition, 2006.

6.5 Legal Issues

The basic legal issues encompassing the issuance of ePassports are privacy of the individual[12]; and the internal security of a State. Ensuring both these are intrinsically and exclusively the responsibility of the State. As for privacy, The Chicago Convention, which established the regulatory framework for international civil aviation, underscores the fundamental aim of States in the context of civil aviation to exchange privileges which friendly nations have a right to expect from each other. In his message to the Conference in Chicago, President Roosevelt said:

> the Conference is a great attempt to build enduring institutions of peace, which cannot be endangered by petty considerations or weakened by groundless fears.[13]

6.6 Privacy

The Chicago Convention, in Article 13 of the Convention provides that the laws and regulations of a Contracting State as to the admission to and departure from its territory of passengers, crew or cargo of aircraft, such as regulations relating to entry, clearance, immigration, passports, customs and quarantine shall be complied with by or on behalf of such passengers, crew or cargo upon entrance into or departure from, or while within the territory of that State. This provision ensures that a Contracting State has the right to prescribe its own internal laws with regard to passenger clearance and leaves room for a State to enact laws, rules and regulations to ensure the security of that State and its people at the airport. However, this absolute right is qualified so as to preclude unfettered and arbitrary power of a State, by Article 22 which makes each Contracting State agree to adopt all practicable measures , through the issuance of special regulations or otherwise, to facilitate and expedite navigation of aircraft between the countries.

The above notwithstanding, there are three rights of privacy relating to the display and storage and use of personal data:

- The right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data;
- The right of an individual to know what data is disclosed, and what data is collected and where such is stored when the data in question pertains to that individual; the right to dispute incomplete or inaccurate data; and

[12]See Abeyratne (2002a). Also by the same author, The Exchange of Airline Passenger Information - Issues of Privacy, *Communication Law*, Vol. 6, No. 5; 2001: pp. 153–162, and also by Abeyratne (2003).

[13]Proceedings of the International Civil Aviation Conference, Chicago, Illinois, November 1–December 7 1944 The Department of State, Vol. 1 at p. 43.

- The right of people who have a legitimate right to know in order to maintain the health and safety of society and to monitor and evaluate the activities of government.[14]

It is incontrovertible that the data subject has a right to decide what information about oneself to share with others and more importantly, to know what data is collected about him. This right is balanced by the right of a society to collect data about individuals that belong to it so that the orderly running of government is ensured.

The data subject, like any other person, has an inherent right to his privacy.[15] The subject of privacy has been identified as an intriguing and emotive one.[16] The right to privacy is inherent in the right to liberty, and is the most comprehensive of rights and the right most valued by civilized man.[17] This right is susceptible to being eroded, as modern technology is capable of easily recording and storing dossiers on every man, woman and child in the world.[18] The data subject's right to privacy, when applied to the context of the full body scanner is brought into focus by Alan Westin who says:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information is communicated to others.[19]

The role played by technology in modern day commercial transactions has affected a large number of activities pertaining to human interaction. The emergence of the information superhighway and the concomitant evolution of automation have inevitably transformed the social and personal life styles and value systems of individuals, created unexpected business opportunities, reduced operating costs, accelerated transaction times, facilitated accessibility to communications, shortened distances, and removed bureaucratic formalities.[20] Progress notwithstanding, technology has bestowed on humanity its corollaries in the nature of automated mechanisms, devices, features, and procedures which intrude into personal lives of individuals. 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.[21] In similar vein, computer records of an air carrier's reservation system may give out details of the passenger's travel preferences, *inter alia*, seat selection, destination

[14]Hoffman (1980), 142.

[15]Abeyratne (2001, 2002b).

[16]Young (1978) at 1.

[17]Warren and Brandies (1890–1891), at 193.

[18]As far back as in 1973 it was claimed that ten reels, each containing 1,500 m of tape 2.5 cm wide, could store a twenty page dossier on every man, woman, and child in the world. See Jones (1973).

[19]Westin (1970), at 124.

[20]Orwell (1984).

[21]For a detailed analysis of the implications of credit cards with respect to the right of privacy see Nock (1993) at 43.

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 else.[22] In similar vein, does it follow that a full body scanning exercise would reveal imperfections of the human body which person would desire to keep private? This scheme of things may well give the outward perception of surveillance attributable to computer devices monitoring individuals' most intimate activities, preferences and physical attributes, leading to the formation of a genuine "traceable society".[23]

The main feature of this complex web of technological activity is that an enormous amount of personal information handled by such varied players from the public and private sector, may bring about concerns of possible "data leaks" in the system, a risk that could have drastic legal consequences affecting an individual's rights to privacy.

At the international level, privacy was first recognized as a fundamental freedom in the *Universal Declaration of Human Rights*.[24] Thereafter, several other human rights conventions followed the same trend, granting to individuals the fundamental right of privacy.[25] The pre-eminent concern of these international instruments was to establish a necessary legal framework to protect the individual and his rights inherent to the enjoyment of a private life.

[22]The paramount importance of airline computer reservation system records is reflected in the world-renowned cases *Libyan Arab Jamahiriya* v. *United Kingdom* and *Libyan Arab Jamahiriya* v. *United States of America* regarding the PANAM 103 accident at Lockerbie, Scotland in 1988, where the International Court of Justice requested air carriers to submit 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 Miller (1971) at 42.

[23]See Scott (1995) at 307; Burnham (1983) at 20. *A contrario* to the argument supported in this thesis that the advancement of technology directly affects the intimacy of individuals. U.S. Circuit Judge Richard Posner favours the idea that other factors, such as urbanisation, income, and mobility development have particularly weakened the information control that, for instance, the government has over individuals: this denotes that individuals' privacy has increased. See Posner (1978) at 409.

[24]The text reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor 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.

[25]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 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.

Privacy represents different things for different people.[26] 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,[27] and culminating in the control over one's personal information.[28] Thus, the conceptual evolution of privacy is directly related to the technological advancement of each particular period in history.

The right of privacy, as enunciated by the United States Judge Thomas M. Cooley, was the right "to be let alone" as a part of a more general right to one's personality. This idea was given further impetus by two prominent young lawyers, Samuel D. Warren and Louis D. Brandeis,[29] in 1890.[30] Before this idea was introduced, the concept of privacy reflected primarily a somewhat physical property or life. The foundations of "information privacy", whereby the individuals would determine when, how, and to what extent information about themselves would be communicated to others, inextricably drawing the right of control of information about oneself,[31] is a cornerstone of privacy. 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.[32] The notion of informational privacy protection, a typically American usage, has been particularly popular both in the United States and Europe, where the term "data protection" is used.[33]

[26]See Regan (1995) at 33; Freund (1971) at 182.

[27]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). See also Cate (1997) at 49. See also Zelermyer (1959) at 16.

[28]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 Simitis (1995) at 447–448. See also Hoffer (2000) at 8.1; Gavison (1980).

[29]See Cooley (1888), as cited in Warren and Brandeis (1980) at 195.

[30]The definition of privacy as the "Right to be Alone" is often erroneously attributed to Warren and Brandeis. See Warren & Brandeis. See Cooley (1888) as cited in Warren and Brandeis (1980) at 195. Additionally the concept of privacy as "the right to be let alone", and "the right most valued by civilized man: was embraced by US courts in the landmark dissenting opinion of Justice Louis D. Brandeis in *Olmsted* v. *United States*. See *Olmsted* v. *United States*, 277 U.S. 438, 478 (1928) [hereinafter *Olmstead*.]

[31]See Westin (1967) at 368. For a similar conceptualisation of privacy, see Fried (1978) at 425.

[32]See Reidenberg (1995) at 498.

[33]The former Privacy Commissioner of British Columbia, Canada, has asserted that privacy was originally a "non-legal concept". See Flaherty (1991) at 833–834. 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 Bennet (1992) at 13.

Self-determination in the right to protect one's privacy was first judicially embraced by the German Bundesverfassungsgericht in 1983.[34] The US Supreme court followed this trend by adopting the principle of privacy self-determination in *DOJ* v. *Reporters Comm. for Freedom of the Press*.[35]

It must be borne in mind that privacy is not an absolute, unlimited right that operates and applies in isolation.[36] It is not an absolute right, applied unreservedly, to the exclusion of other rights. Hence there is frequently the necessity to balance privacy rights with other conflictive rights, such as the freedom of speech and the right to access information when examining individuals' rights *vis-à-vis* the interest of society.[37] This multiplicity of interests will prompt courts to adopt a balanced approach when adjudicating on a person's rights, particularly whose interests of a State are involved.

Since the data contained in equipment such as body scanners may be subject to trans-border storage, there is a compelling need to consider the introduction of uniform privacy laws in order that the interests of the data subject and the data seeker are protected. Although complete uniformity in privacy legislation may be a difficult objective to attain[38] (as has been the attempt to make other aspects of legislation uniform), it will be well worth the while of the international community to at least formulate international Standards and Recommend Practices (in the lines of the various ICAO Annexes) to serve as guidelines of State conduct. After all, as Collin Mellors pointed out:

Under international agreements, privacy is now well established as a universal, natural, moral and human right. Article 12 of the Universal Declaration of Human Rights, Article 17 of the United Nations Covenant on Civil and Political Rights and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, all specify this basic right to privacy. Man everywhere has occasion to seek temporary "seclusion or withdrawal from society" and such arrangements cannot define the precise area of the right to privacy.[39]

It is such a definition that is now needed so that the two requirements of ensuring respect for information about individuals and their privacy on the one hand, and the encouragement of free and open dissemination of trans-border data flows on the other, are reconciled.

In the provision of biometric data, the provider of the information and the receiver thereof are both under obligation to ensure that the data is not used for

[34]WHO Global Influenza Preparation Plan.

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

[36]See Simmel (1971) at 71.

[37]See Halpin (1997) at 111. See also Foschio (1990) at 35. For a comprehensive study on the conflictive interest on privacy and the mass media and the Freedom of Speech, see Pember (1972) at 227; Prowda (1995) 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*.

[38]*Computers and Privacy in the Next Decade*, Lance J. Hoffman ed. op. cit. at 146.

[39]Collin Mellors, *Governments and the Individual- Their Secrecy and His Privacy*, cited in, *A Look at Privacy*, Young (1978), at 94.

any purpose other than clearance of the owner of the information through customs barriers. This information may not later be used for commercial or other gain for instance for advertising purposes (such as using the physical profile of a prominent actor or actress whose biometric information originally given for customs clearance).[40]

The protection of human rights is the most significant and important task for a modern State, particularly since multi ethnic States are the norm in today's world. Globalization and increased migration across borders is gradually putting an end to the concept of the nation State, although resistance to reality can be still seen in instances where majority or dominant cultures impose their identity and interests on groups with whom they share a territory. In such instances, minorities frequently intensify their efforts to preserve and protect their identity, in order to avoid marginalization. Polarization between the opposite forces of assimilation on the one hand and protection of minority identity on the other inevitably causes increased intolerance and eventual armed ethnic conflict. In such a scenario, the first duty of governance is to ensure that the rights of a minority society are protected.

The foregoing discussion addressed the right of privacy of the individual which is paramount over most legal considerations. The only factor that would override this would be the security of State. Inherent to the concept of security of State is State responsibility[41] to its citizens and others who are in its territory. The fundamental issue in the context of State responsibility for the purposes of this article is to consider whether a State should be considered responsible for its own failure or non-feasance to prevent a private act of terrorism against civil aviation or whether the conduct of the State itself can be impugned by identifying a nexus between the perpetrator's conduct and the State. One view is that an agency paradigm, which may in some circumstances impute to a state reprehensibility on the ground that a principal-agent relationship between the State and the perpetrator existed, can obfuscate the issue and preclude one from conducting a meaningful legal study of the State's conduct.[42]

7 Security

It is incontrovertible that in issuing an ePassport, the State concerned ensures aviation security not only in its own territory but also in the territory of the State to which the ePassport holder travels. New and emerging threats to civil aviation are a constant cause for concern to the aviation community. Grave threats such as those posed by the carriage of explosives and dangerous pathogens on board, are real and have to be addressed with vigour and regularity. The leakage of dangerous

[40]See *Gould Estate* v. *Stoddart Publishing Company* (1996) O.J. No. 3288 (Gen. Div)

[41]For an in-depth discussion of State Responsibility see Abeyratne (2009).

[42]Caron (1998) 109, at 153–54 cited in Becker (2006), at 155.

pathogens[43] from laboratories also presents an ominous analogy to the aviation sector in that the same could well occur in the carriage of such dangerous goods by air.[44] Although past instances of the escape of dangerous pathogens are small in number, nonetheless their occurrence and the threat posed to the wellbeing of humanity cannot be underestimated. In 2002 when Anthrax spores escaped from two military laboratories in the United States, the authorities agreed that the leakage was due to a security lapse.[45] In 2003 a string of such leakages occurred in Asia, this time of the SARS virus.[46]

ICAO has been addressing these threats for some time and continues to do so on a global basis, particularly with regard to the impact of unpredictable security measures on passenger confidence in aviation security. There has been much support for this approach because of its value as a deterrent. It has been suggested that States adopt an approach providing for a baseline regime, but with the addition of unpredictable measures, thus achieving a balance between certainty and unpredictability.

The security ensured by the introduction of the ePassport undoubtedly has its genesis in the maintenance of international peace and security is an important objective of the United Nations,[47] which recognizes one of its purposes as being *inter alia*:

To maintain international peace and security, and to that end: take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace.[48]

It is clear that the United Nations has recognized the application of the principles of international law as an integral part of maintaining international peace and security and avoiding situations which may lead to a breach of the peace.

Liability of the manufacturer of the electronic chip, often a private entity, and the State is a significant factor in this equation. Ultimately, even though the chip

[43]Pathogens are microorganisms (including bacteria, viruses, rickettsia, parasites, fungi) or recombinant microorganisms (hybrid or mutant) that are known or are reasonably expected to cause infectious disease in humans or animals.

[44]See Abeyratne (2007).

[45]An year earlier, a covert event occurred in October 2001 when anthrax spores were sent through the mail exposing persons in the eastern USA to contaminated mail resulting in deaths, illnesses and identified exposures to Anthrax. Overt, announced events, in which persons are warned that an exposure has occurred, have taken place in the United States, although most of these were determined to have been hoaxes, that is, there were no true exposures to infectious agents.

[46]The leakages occurred in China, Taiwan and Singapore. See Air-Tight Security, *Intersec*, June 2007 33–35 at 34. See also International Responsibility in Preventing the Spread of Communicable Diseases through Air Carriage - The SARS Crisis. Abeyratne (2002c).

[47]Charter of the United Nations and Statute of the International Court of Justice, Department of Public Information, United Nations, New York, DPI/511 – 40108 (3-90), 100M at 1.

[48]*Id.* at 3.

incorporated in the ePassport is the creation of a public or private entity, is so incorporated in a State document—i.e. the passport, and therefore the State is ultimately liable for defects in the passport. State liability under administrative law can in turn be divided into two limbs: liability for acts of instrumentalities of State; and liability for privatized service providers for whose acts, relating to the provision of technical services, the State would still bear responsibility. The traditional model of administrative responsibility and accountability of the administrative State is based on the premise that Parliament controlled the executive but was in turn controlled by the people. Added to this, the fundamental postulate lay in the overarching principle that the judiciary played its role in keeping instrumentalities and agencies of the State intact. Accountability of the State for its agencies' actions was twofold: one stemming from a statutory power given to that agency by the State; and the other arising from delegation of authority by the State to the agency concerned. In the latter instance, however, the legislature could intervene and share some control of the agency. This gave rise to the inexorable principle that administrative law and judgments of courts on such agencies could be involved only in the former instance, when the State had provided a statutory base for a private agency or entity. In the 1983 British case of *O'Reilly & Mackman*,[49] the House of Lords limited the circumstances in which a public law remedy, such as a declaratory judgment or injunction, could be brought outside of Section 31 of the *Supreme Court Act* of 1918, which prescribed instances of legal actions to be brought against the State for an act of its statutory agent. This is notwithstanding the fact that Section 21 of the Crown Proceedings Act 1949 allows the Court in civil proceedings to issue a declaratory order against the State, although there could be no injunction specific performance orders against a State. Furthermore, a later case established that although the claim for judicial review might be brought against the Crown, the Crown's involvement is merely nominal and the ultimate dispute would be between the claimant and the defendant.[50] It is with the 1990 decision in the *Factorframe* Case[51] where Lord Bridge stated that injunctive relief against the Crown or its officers was not possible.

In the instance of a privatized service provider, the situation calls for a discussion of the reasons for privatization leading to the legal nature of a privatized entity.[52] The reasons for privatization could well range from improvement of efficiency to reducing government involvement in industrial decision making. The corollaries to privatization are often the widening of share ownership; encouraging share ownership by employees; providing more flexibility to pay policies; and enhancement of economic freedom. There could be two types of privatized service providers: the first being large companies which were once instrumentalities

[49][1983] 2. A.C. 237.

[50]*R.* (on the application of *Ben-Abdelaziz and Kugwa*) v. *London Borough of Hackney and the Secretary of State for the Home Department* [2001] 1 W.L.R. 1485, para 29.

[51]*R.* v. *Secretary of State ex parte Factorframe Ltd.* [1990] 2 A.C. 85.

[52]For a detailed discussion of the legal liability of States and of a privatized service provider see Abeyratne (2004).

of state, which, even after privatization, do not possess potential for undue competition in the market. These would easily transit to a position in which large companies had been private in the first place, and would not be subject to principles of public law. The second category of the privatized service provider is one which has market power and consequent potential for untrammelled competition. In such cases, the State may regulate the provider by bringing it under the administrative purview of a State agency. These privatized bodies may be vulnerable under public law through the agencies having administrative control over them.

One of the analogies in the United Kingdom of a privatization of a utility can be observed in the legislative initiative of 1984 with the adoption of the *Telecommunications Act* which brought about the privatization of a major public utility.[53] The 1984 legislation privatized the public corporation *British Telecom* (BT) and abolished BT's monopoly in providing telecom services, thus opening the doors to competition. The Director General of Telecommunications, established by the Act, can grant licenses to operators of telecom systems. The Director General is also empowered to refer a matter to the *Monopolies and Mergers Commission,* particularly on issues related to public interest such as pricing. If this particular feature were to be applicable to a privatized air navigation service provider appointed under Statute, there would be the interesting consideration under public law whether that provider complied with Article 15 of the Chicago Convention[54] on charges for services.

The operation of the administrative process in a State becomes somewhat complex when viewed in the context of competition policy where the State takes measures to curb the ill-effects on society of monopolies and cartels. An initial difficulty that arose was the nineteenth Century control of trade, which was aimed at promoting competition proved counterproductive, resulting in controlling competition. This difficulty was compounded by the early twentieth Century State policy of reluctance to interfere with citizens striking bargains for their benefit.[55] However, after World War 1, some British Governmental measures introduced comprehensive control of market power.[56]

British legislators can be proud of three legislative stages of unfair competition control. The first came in the form of the 1948 *Monopolies and Restrictive Practices (Inquiry and Control), Act* which devolved regulatory responsibility on an

[53]From 1912 until 1981 telecommunications are the responsibility of the Post Office. The 1981 legislation represented telecommunications from KP. Services and established British Telecom as a public corporation.

[54]Article 15 provides that every airport in an ICAO contracting State which is open to public use by its national aircraft shall likewise be open under uniform conditions to aircraft of all other Contracting States. The like uniform conditions shall apply to the use, by aircraft of every Contracting State, of all air navigation facilities, including radio and meteorological services, which may be provided for public use for the safety and expedition of air navigation services. Article 15 also provides that charges applicable to a foreign carrier for the provision of the air navigation services shall not be higher than those imposed on a carrier bearing the service provider State's nationality.

[55]*Mogul SS. Co. Ltd.* v. *McGregor Gow* [1892] A.C. 25. See also *Sorrell* v. *Smith* [1925] A.C. 700.

[56]Committee on Trusts Cmd. 9236 (1918).

agency—the Monopolies and Restriction Practices Commission (MRPC)—a body outside the normal departmental framework. The second stage commenced with the 1956 *Restrictive Trade Practices Act* which addressed the competitive threat of cartels and the *Restrictive Practices Court* was established to adjudicate an anti-competitive and privy issues. The third stage took on with the exPANsion of the *Monopolies Commission* which investigates monopolies issues. Merger irregularities were added to the jurisdiction of the Commission with the *Monopolies and Mergers Act* of 1968. The 1980 *Competition Act* which followed gave the Commission power to investigate particular anti-competitive practices. The final stage of the evaluation demarcates choice of institutions to investigate and adjudicate on anti-competitive practices. From an administrative perspective, the citizen has been known to challenge these State instrumentalities,[57] the most notable of which has been the challenge offered to the various governmental institutions created under Statute to define their extent of duty to give reasons for competition legislation.[58]

A Government's approach to regulation of a public utility, whether public or privatized, is usually based on the public interest rationale where individual consumer choice will determine the demand and supply for goods and their pricing and quantity.[59] In the United Kingdom, these factors are intrinsically related to transparency, accountability, proportionality, consistency and targeting.[60]

The foremost necessity is to establish a strong security culture in every State. For this, there must be a clear definition of State responsibility and accountability brought to bear by a close and unbreakable link between government and industry stakeholders. A security culture would make States aware of their rights and duties, and, more importantly, enable States to assert them. Those who belong to a security culture also know which conduct would compromise security and they are quick to educate and caution those who, out of ignorance, forgetfulness, or personal weakness, partake in insecure conduct. An ePassport must necessarily be the result of efficient and fail-safe organizational arrangements. It should be tested at border control by trained professionals.

eGovernment and eID are the bare essentials for State security. The digital economy has also brought much facilitation that helps the world move to paperless processes which result in greater economy and streamlined processes. However, there must essentially be global harmonization in this process. In this regard ICAO has made remarkable progress in advancing its MRTD programme to the level it is at now. If harmonization means ensuring consistency between global practices, standardization means compliance with international Standards. There is no room for doubt that both harmonization and globalization are needed in this context.

---

[57]See *R*. v. *Monopolies and Mergers Commission Exp. Elders* 1XL Ltd. [1987] 1. W.L.R. 1121. Also *R.V.M. & M. C Exp. Mathew Brown plc* [1987] 1 W.L.R. 1235.

[58]*R*. v. *Secretary of State for Trade Industry* Ex parte Lonrho plc [1989] 1 W.L.R. 325.

[59]Ogus (1994) Charter.

[60]See Better Regulation Guide, UK Cabinet Office (1998).

References

Abeyratne RIR (2001) The exchange of airline passenger information - issues of privacy. Commun Law 6(5):153–162
Abeyratne RIR (2002a) Intellectual property rights and privacy issues: the aviation experience in API and biometric identification. J World Intellect Property 5(4):631–650
Abeyratne RIR (2002) Attacks on America - privacy implications of heightened security measures in the United States, Europe, and Canada. J Air Law Commerce 67(1)
Abeyratne RIR (2002c) Transportation Law J 30(1):53–80
Abeyratne RIR (2003) Profiling of passengers at airports - imperatives and discretions. European Transport Law XXXVIII(3):297–311
Abeyratne RIR (2004) Privatization of Hong Kong international airport: some legal and economic issues. Asia Pacific Law Rev 12(1):31–51
Abeyratne RIR (2007) The safe carriage of dangerous pathogens by air: legal and regulatory issues. Eur Transp Law XLII(6):689–704
Abeyratne R (2009) Principles of responsibility for private acts of terrorism. Bar Assoc Law J XV:55–64
Becker T (2006) Terrorism and the state, Hart monographs in transnational and international law. Hart Publishing, Oxford
Bennet CJ (1992) Regulating privacy. Cornell University Press, Ithaca
Burnham D (1983) The rise of the computer state. Random House, New York
Caron DD (1998) The basis of responsibility: attribution and other trans-substantive rules. In: Lillich RB, Magraw DB (eds) The Iran-United States claims tribunal: its conclusions to state responsibility. Transnational Publishers, Hudson
Cate FH (1997) Privacy in the information age. Brookings Institution Press, Washington, DC
Cooley TM (1888) A treatise on the law of torts, 2nd edn. Callaghan, Chicago
Flaherty DH (1991) On the utility of constitutional rights to privacy and data protection. Case W Res 41:831
Foschio LG (1990) Motor vehicle records: balancing individual privacy and the public's legitimate need to know. In: Kuferman TR (ed) Privacy and publicity. Meckler, London
Freund PA (1971) Privacy: one concept or many. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton, New York
Fried C (1978) Privacy: economics and ethics a comment on Posner. GA Law Rev 12:423
Gavison R (1980) Privacy and the limit s of the law. Yale Law J 89:421
Halpin A (1997) Rights & law analysis & theory. Hart Publishing, Oxford
Hoffer S (2000) World cyberspace law. Juris Publishing, Huntington
Hoffman LJ (ed) (1980) Computers and privacy in the next decade. Academic, New York
Jones RV (1973) Some threats of technology to privacy, privacy and human rights. In: Robertson AH (ed) Presented at the third colloquy about the European convention on human rights, Manchester University Press, Brussels, 30 September–3 October 1970
Miller AR (1971) The assault on privacy. The University of Michigan Press, Ann Arbor
Nock SL (1993) The costs of privacy. Aldine De Gryter, New York
Ogus A (1994) Regulation, legal form and economic theory. Oxford University Press, Oxford
Orwell G (1984) Nineteen eighty-four. Clarendon, Oxford
Pember DR (1972) Privacy and the press. University of Washington Press, Seattle
Posner R (1978) The right of privacy. GA Law Rev 12(3):393
Prowda JB (1995) A layer's ramble down the information superhighway: privacy and security of data. Fordham Law Rev 64:738
Regan PM (1995) Legislating privacy. The University of North Caroline Press, Chapel Hill
Reidenberg JR (1995) 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. Iowa Law Rev 80:497

Scott GG (1995) Mind your own business – the battle for personal privacy. Insight Books, New York
Simitis S (1995) From the market to the polis: the EC directive on the protection for personal data. Iowa Law Rev 80:445
Simmel A (1971) Privacy is not an isolated freedom. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton, New York
Warren SD, Brandeis LD (1980) The right of privacy. Harv Law Rev 4(5):193
Warren SD, Brandies LD (1890–1891) The right to privacy. Harv Law Rev 4:193
Westin A (1967) Privacy and freedom. Atheneum, New York
Westin AF (1970) Privacy and freedom. Bodley Head, London
Young JB (ed) (1978) A look at privacy. Privacy, Willey, New York
Zelermyer W (1959) Invasion of privacy. Syracuse University Press, Syracuse