J Transp Secur (2013) 6:27–42
DOI 10.1007/s12198-012-0101-z

The ePassport — new technology to counter security threats

Ruwantissa Abeyratne

Received: 23 October 2012 / Accepted: 29 October 2012 / Published online: 11 November 2012

Abstract The ePassport is the culmination of a sustained process of development of technical specifications for machine readable travel documents (MRTD). It introduces a new dimension to aviation security in that, within the conventional machine readable passport with its machine readable zone, an additional layer of verification of information contained in an electronic chip is placed, which verifies the information in the passport's machine readable zone by the use of a special reader. Much research has gone into the areas of the technology and verification in the development of the ePassport. At a Symposium held at the International Civil Aviation Organization in early October 2012, the ePassport was subjected to much discussion by the various experts gathered from across the globe. This article discusses these deliberations and places them against the backdrop of the privacy of the individual and aviation security law.

Keywords Biometric indentification · Public key infrastructure · Cryptographic technology · Privacy · State responsibility · MRTD Symposium · ICAO · ePassport

Introduction

Over 104 States are currently producing and using ePassports and there are approximately 400 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

R. Abeyratne (✉)
International Civil Aviation Organization, Montreal, Quebec, Canada
e-mail: tabeyratne@icao.int

should be issued in accordance with the technical specifications approved by the International Civil Aviation Organization (ICAO).[1] 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 recent Symposium on machine readable travel documents, biometrics and security standards held at ICAO on 10 to 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]

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 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

[1] ICAO is the specialized agency of the United Nations handling issues of international civil aviation. ICAO was established by the Convention on International Civil Aviation, signed at Chicago on 7 December 1944 (Chicago Convention). One of the overarching objectives of ICAO, as contained in Article 44 of the Convention is to foster the planning and development of international air transport so as to meet the needs of the peoples for safe, regular, efficient and economical air transport. ICAO has 191 member States, who become members of ICAO by ratifying or otherwise issuing notice of adherence to the Chicago Convention. See ICAO Doc 7300/9 Ninth Edition 2006.

[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

[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.

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 fourfold: 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 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] Machine Readable Travel Documents Part 1 Volume 2, *Supra* note 2 at Page II-3 at Paragraph 4.1.

[7] The Chicago Convention, *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, b)

[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.

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, 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 ten years.

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

[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, *Supra* Note 1, 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.

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 natonality 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 is 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.

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,[13] 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" (The Department of State 1944).

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

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

[12] See (Abeyratne 2002a, b). Also by the same author, The Exchange of Airline Passenger Information - Issues of Privacy, *Communication Law*, Vol.6, No.5; 2001: p. 153–162, and also by Abeyratne, Profiling of Passengers at Airports - Imperatives and Discretions, *European Transport Law*, Vol.XXXVIII, No.3; 2003: p. 297–311

[13] *Supra*, note 1.

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:

1. The right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data;
2. 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
3. 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. [Hoffman (1980)]

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.[14] The subject of privacy has been identified as an intriguing and emotive one.[15] 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 (Warren and Brandies 1890–91). 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.[16] 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. [Westin (1970)]

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. [Orwell (1984)] 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,

[14] (Abeyratne 2001). Ruwantissa I.R. Abeyratne Attacks on America - Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada, *Journal of Air Law and Commerce*, Vol.67, No.1; Winter 2002.

[15] A Look at Privacy, (Young 1978).

[16] 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).

discovering numerous aspects about that particular individual, including, food inclination, leisure activities, and consumer credit behaviour.[17] 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 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.[18] 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".[19]

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*.[20] Thereafter, several other human rights conventions followed the same trend, granting to individuals the fundamental right of privacy.[21] 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.

Privacy represents different things for different people.[22] 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

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

[18] 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 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).

[19] See Scott (1995); 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).

[20] 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.

[21] 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.

[22] See Regan (1995); Freund (1971).

enlarging its scope to include privacy as the individual's decision -making right,[23] and culminating in the control over one's personal information.[24] 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,[25] in 1890.[26] 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,[27] 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 Reidenberg (1995). 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.[28]

Self-determination in the right to protect one's privacy was first judicially embraced by the German Bundesverfassungsgericht in 1983.[29] 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* (1988).

It must be borne in mind that privacy is not an absolute, unlimited right that operates and applies in isolation (Simmel 1971). 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

[23] 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). See also Zelermyer (1959).

[24] 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). See also Hoffer (2000); Gavison (1980).

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

[26] 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). 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*.]

[27] See Westin (1967). For a similar conceptualisation of privacy, see Fried (1978).

[28] The former Privacy Commissioner of British Columbia, Canada, has asserted that privacy was originally a "non-legal concept". See Flaherty (1991). 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.

[29] *Supra*, note 24.

interest of society.[30] 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[31] (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.[32]

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 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).[33]

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.

[30] See Halpin (1997) at 111. See also Foschio (1990). For a comprehensive study on the conflictive interest on privacy and the mass media and the Freedom of Speech, see Pember (1972); Prowda (1995). See also J. Montgomery Curtis Memorial Seminar (1992).

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

[32] Collin Mellors, *Governments and the Individual- Their Secrecy and His Privacy*, cited in, *A Look at Privacy*, John B.Young ed., *Supra*, note 19, at 94.

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

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[34] 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.[35]

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 pathogens[36] 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 (Abeyratne 2007). 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.[37] In 2003 a string of such leakages occurred in Asia, this time of the SARS virus.[38]

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.

[34] For an in-depth discussion of State Responsibility see Abeyratne (2009).
[35] Caron (1998) cited in Becker (2006).
[36] 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.
[37] 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.
[38] 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 (2002a, b).

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,[39] 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.[40]

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 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 two fold: 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*,[41] 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.[42] It is with the

[39] 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), 100 M at 1.
[40] *Id*. at 3.
[41] [1983] 2. A.C. 237.
[42] *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.

1990 decision in the *Factorframe* Case[43] where Lord Bridge stated that injunctive relief against the Crown or its officers was not possible, that the matter was settled.

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.[44] 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 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.[45] 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[46] 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 19th Century control of trade, which was aimed at promoting competition proved counter productive, resulting in controlling competition. This difficulty was compounded by the early twentieth Century State policy of reluctance

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

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

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

[46] 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.

to interfere with citizens striking bargains for their benefit.[47] However, after World War 1, some British Governmental measures introduced comprehensive control of market power.[48]

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 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,[49] 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.[50]

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 (Ogus 1994). In the United Kingdom, these factors are intrinsically related to transparency, accountability, proportionality, consistency and targeting.[51]

Conclusion

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

[47] *Mogul SS. Co. Ltd*. v. *McGregor Gow* [1892] A.C. 25. See also *Sorrell* v. *Smith* [1925] A.C. 700.
[48] Committee on Trusts Cmd. 9236 (1918).
[49] 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.
[50] *R*. v. *Secretary of State for Trade Industry* Ex parte Lonrho plc [1989] 1 W.L.R. 325.
[51] See Better Regulation Guide, UK Cabinet Office (1998).

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.

References

Abeyratne RIR (2001) The exchange of airline passenger information — issues of privacy. Comm 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 (2002b) Transport Law J 30(1):53–80

Abeyratne RIR (2004) Privatization of Hong Kong International Airport: some legal and economic issues. Asia Pac Law Rev 12(1):31–51

Abeyratne RIR (2007) The safe carriage of dangerous pathogens by air: legal and regulatory issues. Eur Transport Law XLII(6):689–704

Abeyratne R (2009) Principles of responsibility for private acts of terrorism. Bar Association Law Journal XV:55–64

Becker T (2006) Terrorism and the State, Hart Monographs in Transnational and International Law. Hart Publishing, p 155

Burnham D (1983) The rise of the computer state. Random House, New York, p 20

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, vol 109. Transnational Publishers, Irvington -on –Hudson, pp 153–154

Cate FH (1997) Privacy in the information age. Brookings Institution Press, Washington, DC, p 49

Cooley TM (1888) A treatise on the law of torts, 2nd edn. Callaghan, Chicago

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

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, p 35

Freund PA (1971) Privacy: one concept or many. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton, New York, p 182

Fried C (1978) Privacy: economics and ethics a comment on posner. GaL Rev 12:423–425

Gavison R (1980) Privacy and the limit s of the law. Yale LJ 89:421

Halpin A (1997) Rights & law analysis & theory. Hart Publishing, Oxford, p 111

Hoffer S (2000) World cyberspace law. Juris Publishing, p 8.1

Hoffman LJ (ed) (1980) Computers and privacy in the next decade. Academic, New York, p 142

International Court of Justice (2000) 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)

Jones RV (1973) Some threats of technology to privacy, privacy and human rights, A. H. Robertson ed. (Presented at the Third Colloquy about the European Convention on Human Rights, Brussels, 30 Sept-3 Oct 1970), Manchester University Press

Miller AR (1971) The assault on privacy. The University of Michigan Press, Ann Arbor, p 42

J. Montgomery Curtis Memorial Seminar (1992) The Public, Privacy and the Press: Have the Media Gone Too Far? American Press Institute, p 2

Nock SL (1993) The costs of privacy. Aldine De Gryter, New York, p 43

Ogus A (1994) Regulation, Legal Form and Economic Theory. Oxford University Press, Charter

Orwell G (1984) Nineteen eighty-four. Clarendon, Oxford

Pember DR (1972) Privacy and the press. University of Washington Press, Seattle, p 227

Posner R (1978) The right of privacy. GaL Rev 12(3):393–409

Prowda JB (1995) A Layer's ramble down the information superhighway: privacy and security of data. Fordham L Rev 64:738–769

Regan PM (1995) Legislating privacy. The University of North Caroline Press, Chapel Hill, p 33
Reidenberg (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 L Rev 80:497–498
Scott GG (1995) Mind your own business – the battle for personal privacy. Insight Books, New York, p 307
Simitis S (1995) From the market to the Polis: the EC Directive on the protection for Personal Data. Iowa L Rev 80(445):447–448
Simmel A (1971) Privacy is not an isolated freedom. In: Pennnock JR, Chapman JW (eds) Privacy. Atherton, New York, p 71
The Department of State (1944) Proceedings of the International Civil Aviation Conference, Chicago, Illinois, November 1-December 7 1944 Vol. 1 p. 43
Warren SD, Brandeis LD (1980) The right of privacy. Harv L Rev 4(5):193–195
Warren SD and Brandies LD (1890–91) The right to privacy. Harv Law Rev 4: 193
Westin A (1967) Privacy and freedom. Atheneum, New York, p 368
Westin AF (1970) Privacy and Freedom. Bodley Head, p 124
Young JB (ed) (1978) Privacy. Willey and Sons, New York, p 1
Zelermyer W (1959) Invasion of privacy. Syracuse University Press, Syracuse, p 16